

**EVALUATING PORT SECURITY: PROGRESS MADE  
AND CHALLENGES AHEAD**

---

---

**HEARING**

BEFORE THE

COMMITTEE ON  
HOMELAND SECURITY AND  
GOVERNMENTAL AFFAIRS  
UNITED STATES SENATE  
ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

—————  
JUNE 4, 2014  
—————

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

Printed for the use of the  
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PUBLISHING OFFICE

90-915 PDF

WASHINGTON : 2016

---

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware *Chairman*

CARL LEVIN, Michigan	TOM COBURN, Oklahoma
MARK L. PRYOR, Arkansas	JOHN McCAIN, Arizona
MARY L. LANDRIEU, Louisiana	RON JOHNSON, Wisconsin
CLAIRE McCASKILL, Missouri	ROB PORTMAN, Ohio
JON TESTER, Montana	RAND PAUL, Kentucky
MARK BEGICH, Alaska	MICHAEL B. ENZI, Wyoming
TAMMY BALDWIN, Wisconsin	KELLY AYOTTE, New Hampshire
HEIDI HEITKAMP, North Dakota	

GABRIELLE A. BATKIN, *Staff Director*

JOHN P. KILVINGTON, *Deputy Staff Director*

MARY BETH SCHULTZ, *Chief Counsel*

JASON M. YANUSSI, *Senior Professional Staff Member*

JASON T. BARNOSKY, *Senior Professional Staff Member*

KEITH B. ASHDOWN, *Minority Staff Director*

ANDREW C. DOCKHAM, *Minority Chief Counsel*

PATRICK J. BAILEY, *Minority Counsel*

MARK K. HARRIS, *Minority U.S. Coast Guard Detailee*

LAURA W. KILBRIDE, *Chief Clerk*

LAUREN M. CORCORAN, *Hearing Clerk*

# CONTENTS

Opening statements:	Page
Senator Carper .....	1
Senator Coburn .....	3
Senator Ayotte .....	13
Prepared statements:	
Senator Carper .....	39
Senator Coburn .....	41

## WITNESSES

WEDNESDAY, JUNE 4, 2014

Ellen McClain, Deputy Assistant Secretary for Transborder Policy, Office of Policy, U.S. Department of Homeland Security .....	5
Rear Admiral Paul F. Thomas, Assistant Commandant for Prevention Policy, U.S. Coast Guard, U.S. Department of Homeland Security .....	6
Kevin K. McAleenan, Acting Deputy Commissioner, U.S. Customs and Border Protection, U.S. Department of Homeland Security .....	8
Brian E. Kamoie, Assistant Administrator for Grant Programs, Federal Emergency Management Agency, U.S. Department of Homeland Security .....	10
Stephen Sadler, Assistant Administrator for Intelligence and Analysis, Transportation Security Administration, U.S. Department of Homeland Security ..	11
Stephen L. Caldwell, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office .....	12

## ALPHABETICAL LIST OF WITNESSES

Caldwell, Stephen L.:	
Testimony .....	12
Prepared statement with attachment .....	57
Kamoie, Brian E.:	
Testimony .....	10
Joint prepared statement with attachment .....	42
McAleenan, Kevin K.:	
Testimony .....	8
Joint prepared statement with attachment .....	42
McClain, Ellen:	
Testimony .....	5
Joint prepared statement with attachment .....	42
Sadler, Stephen:	
Testimony .....	11
Joint prepared statement with attachment .....	42
Thomas, Rear Admiral Paul F.:	
Testimony .....	6
Joint prepared statement with attachment .....	42

## APPENDIX

Additional statements for the Record:	
Hon. Janice Hahn, U.S. House of Representatives .....	130
Kurt J. Nagle, President, American Association of Port Authorities .....	133
American Trucking Associations, Inc. ....	138
Colleen M. Kelley, National President, National Treasury Employees Union .....	144
Henry H. Willis, RAND Corporation .....	149

IV

	Page
Responses to post-hearing questions for the Record from:	
Ms. McClain .....	157
Admiral Thomas .....	165
Mr. McAleenan .....	175
Mr. Kamoie .....	187
Mr. Sadler .....	194

## **EVALUATING PORT SECURITY: PROGRESS MADE AND CHALLENGES AHEAD**

**WEDNESDAY, JUNE 4, 2014**

U.S. SENATE,  
COMMITTEE ON HOMELAND SECURITY  
AND GOVERNMENTAL AFFAIRS,  
*Washington, DC.*

The Committee met, pursuant to notice, at 10:32 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Thomas R. Carper, Chairman of the Committee, presiding.

Present: Senators Carper, Coburn, and Ayotte.

### **OPENING STATEMENT OF CHAIRMAN CARPER**

Chairman CARPER. Good morning, everyone. We are happy to welcome you today and thank you for joining us.

Dr. Coburn and I have called this hearing, and this is a hearing he has had a whole lot of interest in. I have, too. It is a shared interest. But, we want to take a look at the current state of port security in these United States of America. We want to find out if we are heading in the right direction. I hope we can also focus on the work that needs to be done over the next few years to try to ensure that our port security efforts maintain the proper balance between security, safety, and trade facilitation. It is important, because our focus as a Congress cannot solely be on security, but also on maintaining and enhancing our economic competitiveness.

As we all know, port security is no easy job. It involves the maritime security provided by the United States Coast Guard (USCG) when its men and women patrol our coasts and our waterways. It involves the physical security of port facilities like the ferry terminal in Lewes, Delaware, or an energy refinery along the Gulf of Mexico or Delaware City, Delaware, that is safeguarded by State and local authorities. It involves the cargo security provided by the U.S. Customs and Border Protection (CBP), which screens cargo to prevent dangerous goods from entering the United States while also facilitating the flow of trade and transportation.

That last part is a particularly important piece. And, even as we build and maintain strong layers of port security, we need to take care not to impede transportation or commerce. Our ports and waterways are the lifeblood of our economy. I am told that more than 95 percent of all U.S. trade is handled by our seaports. And these ports account for over 30 percent of U.S. gross domestic product (GDP). That is more than \$5 trillion in trade each and every year.

As the former Governor of Delaware and someone who was ultimately responsible for running a major port, the city of Wilmington

owned and ran that Port of Wilmington for many years. They ran out of money and the State had some money, so we took it over when I was Governor. This is something I know a little bit about, but care a whole lot about.

The Port of Wilmington, located along the Delaware River in the northern part of my State—it is just south of Philadelphia—is the No. 1 seaport in North America, believe it or not, for the importation of fresh fruit, bananas, and juice concentrate. If you had a banana this morning for breakfast, it probably came through the Port of Wilmington. We call our port—our nickname is “Top Banana,” the “Top Banana Port.”

The Port of Wilmington is not just important for the State of Delaware, where it serves as a key economic engine in New Castle County. It is also a key port for the entire United States. So, protecting our ports, safeguarding our economic opportunity, is a responsibility that we take very seriously.

As the Government Accountability Office (GAO) and other experts have noted, U.S. port security has come a long way. Shortly after September 11, 2001, the Maritime Transportation Security Act of 2002 (MTSA) became law and empowered the Coast Guard with new authorities to ensure commercial vessels and port facilities meet minimum security standards. A few years later, the Security and Accountability for Every (SAFE) Port Act of 2006 authorized key cargo and supply chain security programs enforced by U.S. Customs and Border Protection. Since that time, these cargo security programs have matured and taken root. Not only that, many of our international trading partners and international trading security organizations have created similar security programs emulating the Department of Homeland Security’s (DHS) good work.

But, we should not and we cannot stop here. We want to use this hearing as an opportunity to explore how the threat to ports has evolved and what the next steps for DHS should be. I also do not want to imply that there is no room for improvement. As I frequently say, everything I do, I know I can do better. I think that is true for all of us, and I think that is true for the way we handle port security.

In a recent letter to the Congress, our new Secretary, Jeh Johnson, indicated he believed the 100 percent scanning mandate for inbound cargo shipping containers was impractical, and not the best use of taxpayer resources. If that is the case, we must look for a better way to address security risks while preserving the necessary speed of moving containers through our ports. So, I welcome the Secretary’s pledge to make a good faith effort to improve the Department’s capabilities without getting in the way of legitimate flow of trade. I look forward to discussing this issue with some of our witnesses today.

I also look forward to hearing how the Department of Homeland Security plans to address emerging threats, how it can make programs more effective and efficient, and how the agencies represented here today can work with international organizations and our foreign partners to raise the global standard for port security.

As you can see from our lineup of witnesses—it is quite a lineup—port security is a team sport. It is a perfect example of why bringing all these agencies together into the Department of Home-

land Security was the right thing to do. The components present here today work seamlessly with one another to develop and implement the Department's layered risk-based strategy for port security. From the Coast Guard to Customs and Border Protection, Transportation Security Administration (TSA), Federal Emergency Management Agency (FEMA), and DHS's Office of Policy, each of you play a critical role and you have to work together. So do we.

I am also glad we have GAO here with us today. We are always happy to have GAO with us. You have done a whole lot of work in this area. We are grateful for that and we will be looking to you for further help.

Again, thanks to everyone for coming. As Dr. Coburn knows, we are going to start voting in a little bit and we are going to do one of those deals that we have perfected, where voting starts and maybe he will go vote the first time, and when he has voted, he will come back and I will go vote, and then we will just swap back and forth. Hopefully, we will be able to keep going and make it all work and be done in a punctual way.

But, this is important. We are happy that you are here. Let me just now turn to Dr. Coburn, just to thank him for insisting that we have this hearing and make this a priority.

#### **OPENING STATEMENT OF SENATOR COBURN**

Senator COBURN. Thank you, Mr. Chairman.

First of all, welcome to all of you. This is an interesting area for us to be talking about. Sitting on the Intelligence Committee, our threats are greater, not less, in terms of risks, and getting it right is important.

One of the commitments I made to Congresswoman Janice Hahn from L.A.—she has the L.A. port, which is one of our busiest, biggest, and probably greatest vulnerability in terms of ports—that we would have this hearing and do the oversight that is necessary to try to improve what we are doing.

So, Mr. Chairman, I would like unanimous consent to put her testimony in the record.<sup>1</sup> The House is out this week, and we would not have scheduled this hearing at this time had we known that, but we did and I am happy that we are having the hearing. So, I would ask unanimous consent to have her testimony included in the record.

Chairman CARPER. Happy to include it.

Senator COBURN. I would also note that the House has passed legislation that the Senate has not even taken up or considered, the Gauging American Port Security (GAPS) Act, and what we need to do is address today to find out where our weaknesses are, what we need to improve it. And, as Senator Carper mentioned, the 100 percent scanning obviously is not viable, or may not be viable, but we need to have a better approach than 2 to 4 percent scanning that we are seeing today.

We know that a successful attack on one of our ports would be devastating. The RAND Corporation gave an example that it could have a trillion-dollar effect on our economy. That is a possibility. We cannot stop every attack that is going to come to this country,

<sup>1</sup>The prepared statement of Ms. Hahn appears in the Appendix on page 130.

but we can certainly make it much more difficult and markedly decrease the likelihood. Everybody knows the history of how we came together after 9/11. We created the Port Security Grant Program (PSGP). We mandated 100 percent cargo screening, and the 9/11 Commission recommended that, as well. We also created the Transportation Worker Identification Credential (TWIC), which has had some significant difficulties and is still not implemented.

So, my goal for this hearing is to review all the initiatives that were initially set out, assess how well they are working and whether or not they are working, and determine if our ports are as secure from a potential terrorist attack as we can make them feasibly and economically.

I would say, we have spent \$2.9 billion on the Port Security Grant Program with no metrics to measure whether or not we have actually improved our security. There are no metrics, so we do not know. We spent \$2.1 billion on CBP cargo programs to meet a scanning mandate that we are told will never be met. So, there is \$5 billion we have spent. We have no assessment of what we have gotten for that money. The TWIC Program was intended to create an ID card for transportation workers to enter secure areas, including the ports. We will talk about TWIC, and some of my questions will relate to some of the problems associated with it. In general, I think it is unclear, and, hopefully, this hearing will help us to know how much improvement we have actually made in securing our ports.

So, I, No. 1, want to thank each of you for being here, preparing the testimony, which I have read, and being available. I apologize that we are going to have votes, but we will keep this moving as fast as we can. We have, I think, four votes starting at 11.

With that, Mr. Chairman, thank you, as well, Mr. Top Banana. [Laughter.]

Chairman CARPER. I have been called worse things.

We will make this work. We appreciate, again, all of you being here. I am going to just briefly introduce our witnesses.

Ellen McClain, Deputy Assistant Secretary for Transborder Policy at DHS's Office of Policy, also served as DHS's Assistant General Counsel for Enforcement. She began her career with the U.S. Customs Service, where she served, I believe, as Deputy Associate Chief Counsel, is that right?

Ms. McCLAIN. [Nodding head.]

Chairman CARPER. Rear Admiral Paul Thomas joins us from the Coast Guard, where he is the Assistant Commandant for Prevention Policy. He is a specialist in marine safety, security, and environmental protection, a graduate of the Coast Guard Academy and of the Massachusetts Institute of Technology (MIT), where I am proud to say that one of our boys attended. When I went to Ohio State, I could barely spell MIT. The idea of having a kid that went to school there, I could not imagine. But, congratulations on that. Thanks for your service.

Kevin McAleenan, Acting Deputy Commissioner at the U.S. Customs and Border Protection. Previously, he served as the Acting Assistant Commissioner of the CBP Office of Field Operations, leading the agency's port security and trade facilitation operations.

Brian Kamoie, appointed as the Assistant Administrator for Grant Programs at FEMA in April 2013. Before that, Mr. Kamoie served as Senior Director for Preparedness Policy on the White House National Security Staff from 2009 to 2013.

Stephen Sadler has been the Assistant Administrator for Intelligence and Analysis at the Transportation Security Administration since October 2011. He joined TSA in 2003 and has held several leadership positions. Prior to that, he spent 25 years in the commercial maritime industry.

And, finally, last but not least, Stephen Caldwell. Stephen, nice to see you. He joins us from GAO, where he is Director of Issues on the Homeland Security and Justice Team. Mr. Caldwell has over 30 years of experience at GAO and has worked on numerous reports on port and supply chain security.

Thank you all. Your entire statements will be made a part of the record, and feel free to summarize as you go along. I will ask you, try to stay within about, what did we say, 5 minutes, if you could. If you go way over that, we will have to rein you in. Thank you for joining us.

Ellen, why do you not go ahead.

**TESTIMONY OF ELLEN MCCLAIN,<sup>1</sup> DEPUTY ASSISTANT SECRETARY FOR TRANSBORDER POLICY, OFFICE OF POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY**

Ms. MCCLAIN. Good morning, Chairman Carper, Ranking Member Coburn. I am a career civil servant and testifying before Congress for the first time. As this has long been on my career bucket list, I appreciate this opportunity, along with my colleagues, to testify on a matter of singular importance to the Department, port security.

Since 2007 and the passage of the SAFE Port Act, we now have several key strategic documents that shape and guide our efforts on port security: The National Strategy on Global Supply Chain Security, the Global Nuclear Detection Architecture (GNDA), and the soon-to-be-released 2014 DHS Quadrennial Homeland Security Review (QHSR).

DHS is focused on enhancing port security through prevention, protection, and resilience, pursuant to a risk-based approach. While strengthening the global supply chain system, including the maritime transportation network, we are ever mindful that it is critical to do so by promoting the efficient and secure movement of legitimate goods.

Guided by the principles in these overarching documents, DHS's approach embraces five elements for a layered system of maritime, port, and cargo security.

One, understanding the risk to better defend and protect against radiological and nuclear risks.

Two, obtaining advance information and using advance targeting techniques.

Three, increased collaboration with other Federal agencies, foreign governments, and private stakeholders.

<sup>1</sup>The joint prepared statement of Ms. McClain, Admiral Thomas, Mr. McAleenan, Mr. Kamoie and Mr. Sadler appears in the Appendix on page 42.

Four, implementing strong domestic security regimes.

And, five, promoting preparedness by sustaining grant programs.

Within this strategic context, DHS can point to several key developments in the past 7 years: Risk assessments to aid us in understanding the threat environment and prioritization of resources; Significant progress with international and private partners to incorporate risk management principles and leverage Trusted Trader Programs; The assessment of more than 1,500 foreign ports, 200 alone in 2013, under the International Port Security Program; Establishment of 360 comprehensive Port Security Plans by port operators; And, grant awards to achieve interoperable communications, installation of surveillance cameras at port facilities, and funding for other similar physical security equipment and projects.

Looking forward, we face challenges of increased trade from the expansion of the Panama Canal and increased activity in the Arctic. With increasing trade and shifting trade patterns, we must also confront aging infrastructure for a broad range of DHS assets, from Coast Guard cutters to X-ray and radiation and nuclear detection inspection systems. In forging the path for progress, DHS will concentrate on improving information collection, targeting, and dissemination, expanding global capacity to secure the supply chain, and addressing risk across all modes of transportation.

With a continued focus on enhancing the capabilities of our components and our partners to address current and future challenges to securing our ports, DHS will continue to dedicate substantial attention and resources to implementing a layered risk management approach to security across all transportation pathways in an efficient and cost-effective way and building essential partnerships at home and abroad.

Thank you again for the opportunity to testify about DHS's progress on enhancements to port security. I will be happy to entertain any questions.

Chairman CARPER. Good. Thanks, and we are going to have some, so thank you.

Ms. McCLAIN. Thank you.

Chairman CARPER. Thanks for your testimony.

Admiral Thomas, please proceed.

**TESTIMONY OF REAR ADMIRAL PAUL F. THOMAS,<sup>1</sup> USCG, ASSISTANT COMMANDANT FOR PREVENTION POLICY, U.S. COAST GUARD, U.S. DEPARTMENT OF HOMELAND SECURITY**

Admiral THOMAS. Thank you, Chairman Carper, Dr. Coburn, and thank you both for your continued support of our Coast Guard and the opportunity to discuss this really important topic with you this morning.

The Coast Guard, in coordination with the other Department of Homeland Security components, the interagency, and the industry, implements a layered maritime security system. Our goal is simple. We want to detect, interdict, and mitigate threats as far from our shores as possible.

<sup>1</sup>The joint prepared statement of Ms. McClain, Admiral Thomas, Mr. McAleenan, Mr. Kamoie and Mr. Sadler appears in the Appendix on page 42.

And, we accomplish this through the layered system that is depicted on the slide before you and displayed to my left.<sup>1</sup> As you can see on the slide, maritime security of U.S. ports does not start and finish in the United States. Rather, the opposite is true. The security of our ports begins in foreign ports, at foreign facilities and terminals. This is the first layer of our integrated system.

The Coast Guard's International Port Security Program conducts assessments of foreign ports to ensure they meet international security standards and to build the capacity of our trading partners. So, just as you cannot enter U.S. airspace unless the flight originated from an airport that meets minimum security standards, you cannot enter U.S. seaports unless that voyage originated from a foreign port that meets security standards as certified by the Coast Guard.

Additionally, the Coast Guard-led Foreign Port Threat Assessments bring together information from law enforcement and intelligence communities to assess the level of governance, crime, terrorist activities, and other factors that may help us determine which threats emanate from those ports.

And, finally, overseas activities by our colleagues from the Customs and Border Protection and other DHS components help to ensure the safety and security of cargo and people before they depart foreign ports.

If you look at the next several layers on the slide, the international waters, the U.S. Exclusive Economic Zone, and U.S. territorial seas, I will call these the offshore layer. Our regulations require that each ship en route to a U.S. port provide the Coast Guard at least 96 hours' advance notice of arrival. This notice includes information about the vessel, the cargo, the crew and passengers. Customs and Border Protection also requires advance notice with information about the cargo, the shipper, the consolidator, the receiving agent, among other information. And, other Federal agencies, like the Centers for Disease Control (CDC), may also require advance notice of arrival under certain circumstances.

All of this information is collected and shared at both the national and the port level. It is screened and assessed so that, prior to arrival of any vessel, the Coast Guard Captain of Port has a consolidated, comprehensive assessment of all risks associated with that ship. And, when I say all risks, I mean all risks, everything related to safety, security, and the environment, as diverse as invasive species in ballast water or cargo, or crew members on a watchlist, passengers exhibiting signs of illness, or damage to the ship that might compromise safety or the environment.

The Captain of Port then is able to coordinate a single inter-agency, local, State, and Federal risk mitigation plan for each ship that arrives. For the vast majority of these ships, local coordination is required to plan the necessary control, inspection, or enforcement actions. In some cases, the threat rises to the level that interagency coordination at the national level is required and we activate the Maritime Operational Threat Response Protocols.

In some cases, the risk will be mitigated by interdicting the ship in the offshore zone. In other cases, the ship is allowed to enter the

---

<sup>1</sup>The slide referenced by Admiral Thomas appears in the Appendix on page 56.

port, but is subjected to inspection and oversight prior to beginning cargo or passenger operations. These boardings are most often led by the Coast Guard, but they may include personnel from other Department of Homeland Security components or the interagency who can bring their special capabilities to bear on a given threat.

In all cases, the vessel arrives at a port facility that complies with the requirements of the Maritime Transportation Safety Act and the SAFE Port Act. These facilities, by law, have security staff trained to specific standards. They have an access control system that includes credentials for each employee. They have approved plans in place to prevent and respond to security incidents. And, they execute a declaration of security with the foreign ships, when appropriate, to ensure the security and communications protocol at that ship-port interface are clear.

And then beyond the individual port facilities, the port community as a whole is prepared and resilient and are capable of coordinated port-wide prevention, preparedness, response, and recovery activities. This is due in large part to the combined impact of investment through our Port Security Grant Program, establishment of the Area Maritime Security Communities, and development of the Area Maritime Security Plans (AMSP).

In summary, Mr. Chairman, we have used the authorities in the Maritime Transportation Security Act and the SAFE Port Act to implement a security system that begins in foreign ports, continues in the offshore area as a vessel transits to our waters, and then remains ever vigilant in our ports that have robust interagency, local, State, and Federal coordination to mitigate threats, facilitate commerce, and respond to all incidents.

Thank you. I look forward to your questions.

Chairman CARPER. You took one second too long. [Laughter.]

You are off your game today, huh?

Admiral THOMAS. Yes, sir.

Chairman CARPER. Actually, that is very good. Thanks for that testimony.

All right. Kevin, you are up. Please proceed.

**TESTIMONY OF KEVIN K. MCALEENAN,<sup>1</sup> ACTING DEPUTY COMMISSIONER, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY**

Mr. MCALEENAN. Good morning, Chairman Carper, Ranking Member Coburn. It is a privilege to appear before you again today.

Thanks to your continued support, along with effective collaboration with Federal, international, and private sector partners, DHS and U.S. Customs and Border Protection have made significant advancements in maritime cargo security. CBP has established security partnerships, enhanced targeting and risk assessment programs, and invested in advanced technology, all essential elements of CBP's multi-layered approach to protecting the Nation from the entry of potentially dangerous or volatile shipments, while expediting legitimate and economically vital commerce. I would like to highlight the progress of a few of these efforts for you today.

<sup>1</sup>The joint prepared statement of Ms. McClain, Admiral Thomas, Mr. McAleenan, Mr. Kamoie and Mr. Sadler appears in the Appendix on page 42.

In the first few years after 9/11, CBP created several key programs to enhance our ability to assess maritime cargo for risk, examine shipments at the earliest possible point, and increase the security of the supply chain. The Customs Trade Partnership Against Terrorism (C-TPAT), was established in 2001 in the wake of the 9/11 terrorist attacks. C-TPAT provides facilitation benefits to vetted members of the trade community who volunteer to adopt tighter security measures throughout their entire international supply chain. C-TPAT has grown from seven initial members to over 10,000 members today.

The National Targeting Center (NTC), also started in 2001, has developed world leading capabilities to assess cargo shipments, crew, and travelers for risk before they are laden or board vessels destined for the United States. At the NTC, CBP utilizes the automated targeting system, intelligence, commercial information, and traveler data to identify and mitigate potential threats.

DHS and CBP have also strengthened detection equipment capabilities at domestic seaports. Since 2001, CBP has acquired 1,387 radiation portal monitors and has increased its inventory of large-scale non-intrusive inspection systems from 64 to 314. These valuable systems help CBP officers detect radiological materials, weapons, and illicit substances.

The support of Congress, specifically through the SAFE Port Act, has been a key catalyst in advancing CBP's trade security and facilitation capabilities beyond these signature efforts. The Act codified and made importer security filings mandatory. Building on the 24-hour rule, this program provides CBP additional advanced insight into the supply chain, allowing us to identify potential risks earlier and more accurately.

The Act also codified the Container Security Initiative (CSI). Under CSI, CBP works with foreign authorities to identify and examine potentially high-risk U.S.-bound maritime containers before they are laden on vessels. CBP's 58 CSI ports now pre-screen over 80 percent of all maritime containerized cargo imported into the United States.

CBP will continue to build on our progress by exploring and expanding new roles for industry stakeholders and international partners, such as Trusted Trader Mutual Recognition Agreements. We will continue to refine our targeting to better identify high-risk cargo, and we will work to increase the percentage of containers scanned abroad. And, we will continue to help lead the effort in developing increasingly effective and sophisticated global standards for cargo security. By utilizing risk-based strategies and applying a multi-layered approach, we can focus our resources on the very small percentage of goods or shipments that are potentially high-risk. CBP's use of advance information, technology, and partnerships improves global supply chain integrity and reduces transaction costs for U.S. businesses.

Thank you for the opportunity to testify today. I am happy to answer your questions.

Chairman CARPER. All right. Thank you for that testimony, Kevin.

Brian Kamoie, welcome.

**TESTIMONY OF BRIAN E. KAMOIE,<sup>1</sup> ASSISTANT ADMINISTRATOR FOR GRANT PROGRAMS, FEDERAL EMERGENCY MANAGEMENT AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY**

Mr. KAMOIE. Thank you, Chairman Carper, Ranking Member Coburn. I appreciate the opportunity to be with you and to join my colleagues from the Department to talk about the Port Security Grant Program, which we believe is a critical part of the Department's efforts to enhance the security and resilience of our Nation's ports.

Senator Coburn, as you mentioned, we have invested \$2.9 billion since 2002. And while I agree with you that we certainly can continue to improve our measurement of both the effectiveness of those investments and our administrative management of the programs, we have clear evidence of the value of these investments across the program's priorities, which include maritime domain awareness.

We have invested in over 600 port-wide projects that include port-wide coordination and collaboration, interoperable communications, and surveillance systems that assist in domain awareness. We have invested \$161 million just in interoperable communications. We have also invested in improvised explosive device (IED) capabilities and chemical, biological, radiological, and nuclear capabilities, cybersecurity capabilities as that threat continues to evolve, planning at the port level training and exercises, and, of course, the implementation of the Transportation Worker Identification Card Program.

So, in addition to these programmatic achievements and, for example, just in vessels that patrol our waterways, we have invested in over 500 vessels. In New York City, for example, the Port of New York used vessels, over 30 vessels, the day Hurricane Sandy made landfall and rescued over a thousand people.

So, we know these dollars are making a difference. And, these investments also facilitate increased partnerships, not just at the Federal level with my colleagues here, but at the State and local level and with port owners and operators, and we have seen in a variety of instances—you can assure Congresswoman Hahn that we continue to make investments in the Port of Los Angeles for information sharing and collaboration, and Chairman Carper, in the Port of Wilmington, the investments there, not just in interoperable communications, but in information sharing between the port and the Fusion Center in Delaware that has allowed the building of relationships with State and local law enforcement and the port.

I thought I would also tell you where we are in the fiscal year (FY) 2014 grant cycle. A hundred million dollars was appropriated for the program this year. Applications came in on May 23. The field reviews—as the Admiral mentioned, we work very closely with the Coast Guard. We have a two-tiered review process. Captains of the Port work with the port area, the local and State government, through Area Maritime Security Committees to prioritize projects. Those applications are under that field review right now

---

<sup>1</sup>The joint prepared statement of Ms. McClain, Admiral Thomas, Mr. McAleenan, Mr. Kamoie and Mr. Sadler appears in the Appendix on page 42.

and will be referred for a national panel review here at the headquarters level later this month, and then we expect to announce awards by the end of July.

And so I will close by saying we look forward to the continuing dialogue about how we can continue to make these investments in the most effective and efficient way possible. We think they have made a real difference. And, I look forward to answering any questions you may have.

Chairman CARPER. Good. Thanks. Nice job.

Stephen Sadler, please proceed. Thank you. Welcome.

**TESTIMONY OF STEPHEN SADLER,<sup>1</sup> ASSISTANT ADMINISTRATOR FOR INTELLIGENCE AND ANALYSIS, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY**

Mr. SADLER. Good morning, Chairman Carper, Ranking Member Coburn, distinguished Members of the Committee. Thank you for the opportunity to testify today about the TWIC Program.

TWIC is a fee-based program that provides a uniform, industry-wide, tamper-resistant, biometric credential to eligible maritime workers requiring unescorted access to secure areas of port facilities and vessels regulated under the Maritime Transportation Security Act of 2002.

TSA administers the TWIC Program jointly with the United States Coast Guard. TSA is responsible for enrollment, security threat assessments, and technical systems related to TWIC cards. The Coast Guard is responsible for enforcement of TWIC card use.

Since TSA launched a program in October 2007 at Wilmington, Delaware, we have conducted security threat assessments and issued cards to more than 2.9 million workers, including longshoremen, truckers, merchant mariners, and rail and vessel crews. The TWIC Program is the first and largest Federal program to issue a standard biometric credential for use in diverse commercial settings across the Nation. Working closely with industry and our DHS partners, the TWIC Program has evolved over the years to address concerns over the applicability of Federal smart card best practices to a working maritime environment, such as the requirement for two trips to an enrollment center for card enrollment and activation. TSA reformed the program by launching OneVisit in June 2013 in Alaska and Michigan. This provides workers the option to receive their TWIC through the mail rather than requiring in-person pick-up and activation. Last month, TSA moved from the pilot phase of the program to a phased implementation for all TWIC applicants. We have added call center capacity for applicants checking on their enrollment status. We have enabled web-based ordering for replacement cards. We have increased quality assurance at our enrollment centers. We have opened multi-program enrollment centers across the country to allow individuals to apply for the TWIC, the Hazardous Material Endorsement, and TSA Pre-Check. We will expand the number of TWIC enrollment centers to over 300 this year, adding to the convenience of workers.

---

<sup>1</sup>The joint prepared statement of Ms. McClain, Admiral Thomas, Mr. McAleenan, Mr. Kamoie and Mr. Sadler appears in the Appendix on page 42.

TSA continues to evolve and modernize our credentialing programs through these initiatives, strong collaboration at the Department, partnership with industry, and the support of this Committee.

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

Chairman CARPER. Thank you, Mr. Sadler.

And now, Stephen Caldwell, please proceed.

**TESTIMONY OF STEPHEN L. CALDWELL,<sup>1</sup> DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE**

Mr. CALDWELL. Chairman Carper and Senator Ayotte, thank you for asking GAO to testify on port security.

We have issued almost 100 reports on port security since 9/11. Our most recent comprehensive report on port security was issued in the fall of 2012 to note the 10-year anniversary of the Maritime Transportation Security Act.

Let us start with planning. There was a National Strategy for Maritime Security issued in 2005. GAO reviewed that strategy and its eight supporting plans and generally found they met much of the criteria that GAO has laid out for a good national strategy. We have also looked at some of the more detailed functional strategies, and in some cases, we have found those to be wanting. At the port level, we found that some of the plans specific to the ports have included the SAFE Port Act's requirement that they also cover recovery issues.

Going back to some of the functional plans, we found some deficiencies in those. For example, DHS, after issuing the Small Vessel Security Strategy and laying out an implementation plan for that, has not been tracking the progress of the components in actually implementing it. That leaves some opportunities unrealized due to the lack of disseminating any potential lessons learned or even be able to track their overall progress on that strategy.

In terms of maritime domain awareness, there have been a number of improvements. The Coast Guard through its Common Operating Picture Program, has provided additional data sources to the users; allowed Blue Force Tracking, which is the ability to track our own vessels; and also increased access across the Coast Guard to more users. However, many of the original systems used to increase maritime domain awareness have fallen short of the capabilities that were originally planned for those. Many of these shortcomings are due to acquisition problems that our reports have noted, such as not developing complete requirements at the beginning, not updating cost or schedule baselines, and not monitoring performance through initial operations.

Regarding the security of our domestic ports, DHS components, especially the Coast Guard, have come quite a ways in implementing the Maritime Transportation Security Act. Key provisions of that Act call for security planning at the port, facility, and vessel level. It also calls for the Coast Guard to then inspect those facilities to make sure that those planned security activities are indeed

---

<sup>1</sup>The prepared statement of Mr. Caldwell appears in the Appendix on page 57.

in place. GAO has audited those programs. We have found progress, and most of our recommendations in those areas have been implemented.

But, some areas remain problematic, and as noted in our reports, we have concerns about the Port Security Grant Program and the extent that DHS is monitoring the effectiveness of the actual projects. Going back to 2005, GAO found that the program lacked an adequate risk assessment process. It also lacked a mean to measure the effectiveness of the projects and the grants. Our more recent work did find that the grants are based on risk using the process that Mr. Kamoie had described here at both the port and the national level.

However, more than a decade after the program's start, there are really no performance measures in place to determine whether the program at the port or facility level has improved security. In fact, in many cases, FEMA lacks project-level visibility to know whether the projects were, indeed, implemented as described.

Regarding global supply chain security, there has also been a lot of progress, especially by CBP. We have reviewed these programs and noted that their management and operations have matured over time. We concur with CBP that implementing 100 percent scanning, as defined in the SAFE Port Act and 9/11 Act, is extremely challenging. However, we are less convinced that the existing risk-based program does not have room for improvement. Our recent reports have found that CBP has not been timely in terms of measuring the effectiveness of its targeting system or evaluating the supply chain risks in foreign ports, including CSI ports. We did see the May 5 letter from the Secretary to you, Mr. Chairman, and note that both of those issues are discussed as potential improvements.

In closing, GAO will continue to review port security programs for Congress, for this Committee and others. For example, we have ongoing work on port cybersecurity as well as the disposition of high-risk containers.

That concludes my remarks. I am happy to answer any questions. Thank you.

Chairman CARPER. Good. Thanks so much for that testimony.

Senator Ayotte, nice to see you, and why do you not lead us off.

#### **OPENING STATEMENT OF SENATOR AYOTTE**

Senator AYOTTE. Thank you, Mr. Chairman. I appreciate it.

I just wanted to get a followup, Assistant Administrator Sadler, and certainly Mr. Caldwell, about the TWIC Program. So, you testified about the OneVisit pilot, and now it is going to a nationwide mailing system. So, how do you assess it is going, and are you able to do this without concerns about fraud? So, just can you give us a quick update? Obviously, I appreciate the steps you have taken on this, but just in terms of substance.

And then I would like to hear from Mr. Caldwell about how effective you think, overall, the TWIC Program is in helping protect port security and what other—I mean, GAO has been quite critical in past reports about what we need to do to improve this program and its effectiveness. So, that is really the issue I was hoping to get a little more insight on. Thank you.

Mr. SADLER. Good morning, Senator. So, we started the pilot for TWIC OneVisit last year, or 2012 to 2013, in Alaska and Michigan. And then what we did, as we transitioned to our new technical system, we started the implementation nationwide. So, we started implementing the OneVisit in May of this year, May 12. So, we plan to have a phased schedule to implement it across the Nation and we should have it done by this summer.

So, we think it is going fairly well. We do mail the cards out. I believe we have about 3,000 cards for TWIC OneVisit right now that have been mailed out of about 5,000 enrollments. So, what we do is we send the card out separately and then we send the PIN in a different letter. So, we try and send them out in two different letters.

Senator AYOTTE. So, you have not seen fraud yet on that program?

Mr. SADLER. On the mailing itself?

Senator AYOTTE. Yes.

Mr. SADLER. Not yet, Senator.

Senator AYOTTE. OK.

Mr. SADLER. But, we are still in the early stages of the implementation.

Senator AYOTTE. OK. Thank you.

And, Mr. Caldwell, I know we are in the middle of a vote, so I just wanted to get a quick thought on—one of the things I think we have worried about overall about the TWIC Program, is it making us more secure? Are we improving this system so that we can have some reliability with it?

Mr. CALDWELL. Well, two things. The TWIC OneVisit pilot, is a tradeoff between security and convenience. It is more convenient to use the mail but you are losing at least one of your internal controls of being able to verify the person's identity by having them pick it up in person. Congress directed TWIC to go in that direction and—

Senator AYOTTE. They did—

Mr. CALDWELL [continuing]. So, that is what TSA did.

Senator AYOTTE. But, it is also good for us to followup—

Mr. CALDWELL. Yes.

Senator AYOTTE [continuing]. To make sure that we did not—that the choice we made there, that I was obviously a supporter of—

Mr. CALDWELL. Yes.

Senator AYOTTE [continuing]. That we make sure that we are following up on it, as well.

Mr. CALDWELL. Yes. I do think it is a good idea to follow up on that to see if there is fraud.

Senator AYOTTE. But what I am worried about overall is, are we really doing anything with TWIC? I am not trying to be funny about this.

Mr. CALDWELL. Yes.

Senator AYOTTE. I get the goal of it. It makes sense. But, obviously, the concern has been, how are we enhancing port security overall?

Mr. CALDWELL. We have those concerns, as well. We have had concerns with the program pretty much from day one and the ways

it was implemented. For example, the reader pilot that was done recently, we thought the evaluation of that was done quite poorly and left out a lot of things that would be used to evaluate the nature of any problems. What were the problems that were coming up? Was it the card itself? Was it the reader? Was it the person that was manning the security gate? When they did their test of the reader pilot, they did not include this kind of detailed data you need to know to get answers to such questions.

Obviously, there are some additional concerns in terms of the shooting down in Norfolk Navy Base.

Senator AYOTTE. Yes. That was raised in the Commerce Committee.

Mr. CALDWELL. And the Navy now is not accepting TWIC, at least by itself, as an acceptable card to get on that base. So, they had some concerns with it.

There has been an assertion that the TWIC has improved security, and we have seen that reported in the latest DHS report to Congress. But we have not seen strong evidence supporting it in terms of evaluating metrics.

Senator AYOTTE. So, you want better metrics and you want—

Mr. CALDWELL. GAO always wants better metrics, but—

Senator AYOTTE. Yes.

Mr. CALDWELL. But, I suspect we will be asked to look at it again as it continues to be implemented.

Senator AYOTTE. Are we doing better? I mean, that is a good question.

Mr. CALDWELL. Well, compared to nothing, having a pass that is unique, that is used in multiple places and with the background check, is useful. You can have felons because past crimes can be waived, so they still have those cards. But you do not have people getting the cards that have committed espionage against the United States or terrorism crimes. That is a pretty high bar. But one other way to look at it is that TWIC was put in—

Senator AYOTTE. Yes, that would be important.

Mr. CALDWELL. TWIC was put in as part of MTSA, as a series of protections, to prevent a transportation security incident. That is where its a judgment call, about whether someone getting in, committing a crime, committing murder, an whether would that rise the level of a transportation security incident? Not likely.

Senator AYOTTE. If there is anything else you want to add. I know we have to run to vote, but—

Mr. SADLER. Just quickly. The first thing I want to say is, for a TWIC OneVisit, you have to go in and confirm your identity when you go in to—

Senator AYOTTE. The first time.

Mr. SADLER. The first time.

Senator AYOTTE. Absolutely, yes.

Mr. SADLER. You have to do that. The other thing I would say is that this is the first time that the maritime population has been defined. Prior to TWIC, there was no definition as far as I know, and I spent 20 years going in and out of ports. So, I am not sure who knew nationally who was going—

Senator AYOTTE. Who was going in and out of the ports.

Mr. SADLER. And who was not going in.

Senator AYOTTE. We now know that answer.

Mr. SADLER. We now have a population of three million people, and I vetted port workers before TWIC, a name-based vet with information that was submitted by ports. We vetted 900,000 people. We did that prior to the implementation of TWIC as a mitigation strategy. Now, we are up to three million people, all right. So, the first thing is that we have defined the population. We recurrently vet them, every single day.

Senator AYOTTE. Mm-hmm.

Mr. SADLER. We have one common standard—put the biometric aside—one common credential, one common background check. That did not happen prior to the TWIC across the country. And some places, you had to buy a multiple credential within the same State.

Senator AYOTTE. Right.

Mr. SADLER. So, if you went to one port, you had to buy a credential. You went to another port, you had to buy a credential. And, I cannot tell you what the background check was. So, we think there is improvement in security just by virtue of the fact of those things that I just mentioned.

Senator AYOTTE. Thank you and thank you, Mr. Chairman.

Chairman CARPER. Not at all.

I am going to slip out and run and vote and then come back, so Dr. Coburn and I can go back and forth. I just want to telegraph my pitch. When I come back, among the questions I will be interested in asking, so you can be thinking about them, are how do we measure success? I want to see if there is some consensus on how we measure success and if there is some consensus around common metrics. Then, how are we doing? What are we doing especially well? What are we not doing so well? And, finally, I always like to ask, what can we do to help?

All right. Dr. Coburn. Thank you all.

Senator COBURN. [Presiding.] Thank you. Have fun voting.

Let us keep talking about TWIC for a minute. I would just like your assessment on somebody with a TWIC card that gets into a port and shoots people. How does that happen? No system is perfect, and I am not laying blame. I am just saying, how did we miss that?

Mr. SADLER. At the time that individual was vetted, Senator, the standard for manslaughter included all manslaughter, voluntary and involuntary. So, when the individual came through—the crime had been committed in 2005. The conviction occurred in 2008. I believe he served about 800 days on his conviction, so he served about 2½ years. He was released from incarceration in 2011. We encountered him in December 2013. And, based on the standards that we were using at the time, that voluntary manslaughter charge was not a disqualifier. So, he got his card in January 2014.

As far as him using the card at the base, I would defer to the Department of Defense (DOD), but the one point I have to make is that the TWIC in and of itself does not give you access to a port. You have to have the TWIC and you have to have a business need.

Senator COBURN. Yes.

Mr. SADLER. So, we have gone back. We are scrubbing all the cases we had for disqualifications and involuntary manslaughter,

voluntary manslaughter. And, we changed our policy now that if you come in with a voluntary manslaughter charge, that is going to be an interim disqualifier—

Senator COBURN. Yes.

Mr. SADLER [continuing]. Interim, meaning that you are still eligible to appeal. You are still eligible to request a waiver.

Senator COBURN. Right.

Mr. SADLER. You are still eligible to request an Administrative Law Judge (ALJ) review. And, you are eligible to go to court if you do not agree with the finding that we make.

Senator COBURN. OK, great. That is the kind of answer I was wanting.

Talk to me about TWIC readers.

Mr. SADLER. I will defer to my colleague in the Coast Guard, but to Senator Carper's point about what we can do to increase security and how we can be more successful, that is one way we can be more successful, is by implementing the TWIC readers, because we have a biometric credential. We believe that it works. Right now, it is being used as a visual identification card, but it needs to be used as the biometric credential, and it needs to be used on a risk-based basis, as well. So, we believe that it is critically important to install readers in ports.

Senator COBURN. Admiral.

Admiral THOMAS. Thank you, Doctor. I really appreciate the opportunity to answer that question, because as the agency responsible for implementing security at our port facilities, and as a previous Captain of Port myself, I think it is important to recognize that TWIC and the TWIC reader are part of a greater access control system for a facility, which has its own security system, which is in itself part of a greater system to secure our ports and the entire chain that I discussed.

So, when you are going to put an access control system in a facility, you are going to include fences, gates, guards, lights, cameras, a credential of some sort, and in some cases, a biometric reader for that credential. So, it is just a matter of layering the security.

As the Chairman noted in his opening comments, if this was security at all costs, we would have readers everywhere. But, because we are trying to balance, as we should, the risk with the benefit and facilitate commerce, we have done an exhaustive analysis, which I am happy to explain to you, that has ensured that the readers go at the highest-risk facilities. And I think that the Coast Guard's proposed rule puts those readers where the cost-benefit is currently the best. I think as we expand the use of TWIC and TWIC-like credentials beyond the maritime domain, because right now, it is the only place we have transportation credentials, reader costs will come down, card costs will come down, and the cost-benefit may change in a way that it just makes sense to put readers at more facilities. Thank you.

Senator COBURN. Do you have a proposed date where your first round will be completed and then an assessment made of TWIC readers?

Admiral THOMAS. We are currently working on the rule. We put out a Notice of Proposed Rulemaking. We have received about 2,600 comments. So, we are currently working through those com-

ments. We are going to make some adjustments to the rules and we will go through the process. Hopefully, it will be published probably some time next year, and then there will be a 2-year implementation date before the readers have to be in place.

Senator COBURN. So, we are 2½ years away from the completion of what the present plans of the Coast Guard are?

Admiral THOMAS. We are 2½ years or so away from the date that I anticipate readers will be required at certain port facilities.

Senator COBURN. OK. Thank you.

Let me go back for a minute. Ms. McClain, one of your statements in your opening statement was spending money in a cost-effective way. If you all do not have metrics on the effectiveness of grant money that is spent, how do you know it is cost effective?

Ms. McCLAIN. Senator, I appreciate the question. I think it is a little outside my lane. I would prefer to take that question back and get you an answer, working with my colleague from FEMA, on where we are in developing metrics or answering that particular question.

Senator COBURN. Well, I do not think anybody will dispute that we have done some good with the money we have spent, OK. I am not saying that. I am just saying—and anybody can answer this that wants, and I would love for GAO to comment on it, as well. We have a port system where we tier risks and the vast majority of money have gone to tier one ports. And, under the system you are utilizing today, without any recognition of the money that has already been spent, we continue to spend the same money on the same risk because there is no risk reduction recognized in your tiering.

So, if you do not have metrics associated with the money that is being spent in the Port Security Grant Program, when do we stop spending money at tier one ports? In other words, how much is enough, and how do we know when we have the best cost-benefit analysis, the most cost-effective program, based on the risks and mitigation and the other goal that we have, how do we know that if we do not have a metric-based system?

In other words, here is why we are spending this \$2.9 billion. Here is what we are hoping to get, and here is how we are going to measure whether we got it, because there are all sorts of examples—I will not in this hearing—but privately—give you all the lists of money that you spent on stuff that a common sense person would say, does not have anything to do with port security. I mean, I can think of—the two ports we have in Oklahoma, the Port of Muskogee and the Port of Catoosa, and we have two 27-foot boats for the Oklahoma Highway Patrol on that river. And in terms of the risks associated with those ports, those are low priority to me compared to what the higher priority things are on that port, those two ports.

So, my question is, if we do not have metrics to measure, and when we look at this in total—and I think you all have done a wonderful job in terms of laying this out—but, how do we know, and how do we know when to quit spending money that gives us a diminishing return on the Port Security Grant Program?

Mr. KAMOIE. Senator, I am happy to field that question. Improved measurement is absolutely an area where we see a lot of opportunity.

Senator COBURN. But, let me interrupt you there.

Mr. KAMOIE. Please.

Senator COBURN. What is your measurement now?

Mr. KAMOIE. Sure. In fiscal year 2013, we, for the first time, instituted measures related to sustainment of existing capabilities versus building new ones. We took the GAO and Mr. Caldwell's reports and recommendations quite seriously and are looking very closely at what ports are doing with the funding. We, for the first time, in the fiscal year 2012 application cycle are requesting project-level data going in. You probably are aware of the history of the program and the flexibility that had been given at the local level against Area Maritime Security Plans. There remains a lot of flexibility, but we are increasing the oversight to request project-level data up front so that we can start to get that information to form even more effective measures of outcomes.

On the grants management side, Senator, we certainly have measures now, and even over fiscal year 2012, measures of our monitoring. Mr. Caldwell mentioned the level of monitoring. One hundred percent of our Port Security Grants now undergo some level of monitoring. We have a tiered monitoring system where our program staff on a routine basis look at every award, look at the history of the grantee, the history of the outcomes achieved, their financial measures, from draw-down, rate of expenditure, rate of deobligation, and that, then, is reviewed, and we do prioritize based on the risks we see in their management of the grants all the way up to desk reviews, where we request a lot of additional information from grantees, and then site visits.

So, what I would tell you, Senator, is I look forward to continuing to work with you to continue to get the data we need to form more effective measures. I agree with you that everybody can point to the examples, and there are really some stunning examples of how useful and effective this funding has been. But, I think you would also agree with me the plural of anecdote is not data, and we will continue to refine our measures to get that data.

Senator COBURN. Yes. As I noted, I think it has improved, but I think my underlying concern, somebody is going to be sitting up here 10 years from now, and the amount of money to spend on this kind of program is not going to be there. So, how we spend the money today is really important, because there is going to come a time—I will repeat for you, Social Security Disability runs out of money at the end of next year. Medicare runs out of money in 2026. Social Security runs out of money in 2032. By 2030, the entire budget will be consumed of Medicare, Medicaid, Social Security, and the interest on the Federal debt.

So, my questions are all based on the future, and if we spend money really well now, we will not need to be spending money in the future. So, that is the basis of the question. It is not a criticism. It is just that we need the best cost-benefit value for every dollar that you send out in the Port Security grant.

Mr. KAMOIE. We agree with you and we are working with our partners on the Vulnerability Index, which is one of the things you

mentioned, and how do we understand what risk we have bought down, and we will continue to look at that to make sure we are spending the money as effectively as possible.

Senator COBURN. Thank you.

Admiral, one of my concerns, and I cannot go into detail, but let me give you a hypothetical and you give me the answer. Let us say somebody leaves one of our certified ports overseas and arrives here, but in between there and now, something was added to that cargo. Do we have the capability to know that?

Admiral THOMAS. Well, Doctor, I am not exactly sure. If they leave a foreign port—

Senator COBURN. They leave a foreign port that is one of our certified ports, one of our allies, meeting all the requirements that you all have, and someplace between when they left and when they arrived at the Port of Los Angeles, somebody has added a package.

Admiral THOMAS. So, if that occurred at another foreign port, so—

Senator COBURN. No, not in the port—

Admiral THOMAS. Just in transit.

Senator COBURN. In transit.

Admiral THOMAS. Well, the only way that we would be able to determine—a couple things would have to happen. Probably, the entire crew would have to be complicit with this individual that is carrying this out, because it is difficult to access particularly a container in transit without a significant amount of effort, and that would require probably more than one person.

Senator COBURN. Let us not worry about the details of that.

Admiral THOMAS. Sure.

Senator COBURN. Let us say it happens.

Admiral THOMAS. If it happens, the only way we would know is—and, really, this is a better question for my colleague from Customs and Border Protection—would be because the container has been opened and we would be able to determine that, but maybe you can—

Mr. MCALEENAN. Sure. Senator, we have two elements that I think would be germane here. One, the Import Security Filing gives us the stow plan for the vessel, so we know where each container is on a vessel, whether that is going to be accessible during a voyage or not. We do see drug smugglers attempt to use what we call rip loads, where they break the Customs seal, put a load just inside the doors of the container, and lock it back up. That is really only doable on a vessel in transit around the deck area. So, we know which containers could be accessed. And then we do routine seal checks upon arrival to see whether those containers have been tampered with, whether those doors have been opened. So, there are different steps in our layer of processes to address it.

Senator COBURN. Can somebody duplicate counterfeit your seal?

Mr. MCALEENAN. They can try to, yes, and we have detected dozens of attempts to do that pretty effectively.

Senator COBURN. So, they have not been able to do that as of yet?

Mr. MCALEENAN. I will not say, Senator, that—

Senator COBURN. That you are aware of.

Mr. MCALEENAN [continuing]. There have been no successful counterfeit attempts, but we do train our personnel to detect what our seals are supposed to look like, whether they have been tampered with, and there are number sequences and other kind of safeguards in this process.

Senator COBURN. This is a long time ago, but I will just share an experience with you. I bought a company in Puerto Rico, put it into four containers, all the equipment, everything that was there. All four containers arrived at one of my plants here. All the seals were there. And when we opened the containers, everything of significant value that could have been marketed was gone, but the seals were still there. So, the fact is—and that is way before 9/11. That was in the 1970s. But, the fact is that people will try and do it.

I guess my question is really this. Do we have the capability to track ships from the time they leave a port until the time they arrive here and know whether or not they have been boarded or accessed between disembarkment and embarkment here?

Admiral THOMAS. That is a question I probably cannot answer in this venue, sir.

Senator COBURN. Got you. All right. Thank you.

Mr. CALDWELL. Senator, did you want me to touch upon the metrics issue?

Senator COBURN. Yes, please.

Mr. CALDWELL. We have seen a weakness in metrics at the strategic level. Whether it is the national strategy or the more detailed functional plans, we have not seen metrics laid out early as to what the end state is and how we are going to measure that. We have also seen problems, particularly at the program level, because those are easier for GAO to look for and find.

We have found an improvement of the metrics of how the programs are run, i.e., process metrics. One of the first things that we do when we look at a program is ask how the program is being run and obtain those metrics. A lot of times, we will find weaknesses in those process internal controls. Those have improved across the board, and so when I say some of these programs have matured, a lot of this is better management of the program. Where we have not seen large improvements is in the area of actually measuring the results of the program and what they are trying to achieve.

I would also agree with you on the importance of cost-benefit analysis. We will get a push back from the agency that our recommendations could be expensive and they do not have enough money to implement them. But FEMA ends up spending \$3 billion on port security grants. GAO has had an outstanding recommendation for 9 years now, that FEMA come up with performance measures on the Port Security Grants. So, maybe a couple of million dollars to do some analysis to develop those metrics on performance, in hindsight, looks like it might have been money well spent.

One example of cost-benefit analysis having a positive impact involves the advanced spectroscopic portals (ASP) that the Domestic Nuclear Detection Office (DNDO) was developing. The first testing that DNDO did it was very light—it was not very rigorous. We pointed that out. When they did the rigorous testing and then they looked at how much those ASPs would cost compared to the mar-

ginal capability they were going to add, DHS canceled the whole program. They canceled it after spending \$280 million, but eventually, they were planning to spend, \$3 billion, so that was a case where whatever the testing or analysis cost in the end it led to a good result.

Senator COBURN. All right. OK. Let me ask Mr. Kamoie, do you all have plans to reinsert the fiduciary agents into the PSG?

Mr. KAMOIE. We do not, Senator.

Senator COBURN. And why is that?

Mr. KAMOIE. When the fiduciary agent model was used, it was at a time when the appropriations levels for the program were much higher, and was several—I think it was starting in 2007 and after rounds of stimulus funding. The agent model was absolutely necessary to assist the agency in distributing and monitoring the funds.

Over time, however, as the appropriations level has gone down and our internal capability with staffing has increased to manage the program, the fiduciary agent model has become less necessary. And in terms of monitoring performance, there was a varying level of performance by fiduciary agents in monitoring, and so given our increased staffing, our increased capabilities, we think it is more appropriate that we monitor and oversee the grant funding and how it is spent.

The other thing I will say is that the allowability of management and administration costs from the grant program to fiduciary agents of 3 to 5 percent would result, for example, just this year in \$3 to \$5 million in overhead costs that we think are better invested in actual port security projects.

Senator COBURN. Do you have the flexibility under the appropriation bills to use some of that grant money for grant management?

Mr. KAMOIE. Senator, I will have to check the language and get back with you on that.

Senator COBURN. But, would that help you? In other words, rather than spending \$3 to \$5 million on a fiduciary, if we spent an extra \$1 or \$2 million on managing grants, especially cost effectiveness of grants, and then looking at that—I am pleased with the progress that is being made. I just do not think we are there yet, and so I would love to know what we need to do to help you to be able to get to the point where a model for grants at the Federal Government is, the Division of Library and Museum Sciences. If you get a grant from them, you can guarantee that they are going to check on you. They are going to do a metric. They are going to know whether you followed your plan in the grant. And if you are not, they pull the grant and you do not ever get another one again. So, everybody has a different expectation, and so the fact that some grant money is going to things that are not really for security, if you had that reputation, I guarantee you, everything would be put down the way you want it put down, even though you have flexibility.

Mr. KAMOIE. I will absolutely take a look at that. We are willing to learn lessons from wherever we can.

Senator COBURN. They are the best run grant program in the government. It is not big.

Mr. KAMOIE. I appreciate that.

Senator COBURN. The other thing is the spend down. We are still, in terms of what—we have granted, but we have still got a long ways to go on spend down. Where are we on that, and is that because these are long-term programs?

Mr. KAMOIE. So, that is getting better, as well, and early on in the program, when ports were doing larger capital project infrastructure building with multi-phase, complicated projects, it took a long time to spend down. A lot of those projects have been completed and we have taken a number of steps to assist grantees in the spend down. One, we remind them quarterly.

Senator COBURN. Yes.

Mr. KAMOIE. We are in touch, asking them to draw down. Two, we have shortened the period of performance for grants to 2 years.

But, your question was where are we. In August 2012, for—and we can followup in writing with these numbers, but for the program years 2008 to 2011, 80 percent of the available funds were not yet drawn down. A year later, for fiscal year 2008 to 2012—of course, every year, one goes off the books—but, we moved the needle down to 44 percent of funds not being drawn down. And, we did a check at the end of April, and right now, we are at 39.3 percent not yet drawn down from 2008 to 2013.

Senator COBURN. All right. I am going to have to recess this and go vote. Senator Carper will be back in a moment.

Mr. KAMOIE. Thank you, Senator.

[Recess.]

Chairman CARPER. [Presiding.] Let us just see if there is any consensus on the metrics that we are using, how do we measure success. Let us just start with you, Ms. McClain. What are the metrics that we are using or ought to be using, and using that metric or metrics, how are we doing?

Ms. MCCLAIN. Mr. Chairman—

Chairman CARPER. Well, and maybe not so well.

Ms. MCCLAIN [continuing]. I think there are several indicators that evidence success and progress in securing the ports. I would note that in the last 7 years, our relationships, our programs internationally, those global partnerships, the capacity building, the agreements, everything that is necessary to supply the whole global supply chain, I think there have been significant advancements in that area. I also think that our improvements in the advance data and targeting area make us more secure, the Coast Guard's port assessments, 1,500 ports. I think there are a lot of indicators that there is a global recognition of the need to tackle this issue on a broader basis.

Chairman CARPER. All right. Same question, Admiral Thomas.

Admiral THOMAS. Thank you, Mr. Chairman. I was Captain of Port in Galveston, Texas, on September 11, 2001, and then for the 3-years that followed as we scrambled to figure out what it meant to secure our ports, and so from my perspective, it is clear that we have achieved a lot. But, I think one of the first things we did, and Mr. Caldwell mentioned the strategies that were out there, we recognized that in order to build a secure port, we had to first build the regimes. We had to do that locally. We had to do it nationally. We had to do it internationally. Then we had to build awareness

so we could figure out what was going on and be able to pick out anomalies. And then we needed the capability to respond to those anomalies.

So, if you look at those three building blocks and you compare to where we were on September 11, 2001, to where we are today, it is clear there has been progress, and there are clear metrics within each of those.

So, with regard to regimes, certainly thank you to the Congress for the Maritime Transportation Security Act and the SAFE Port Act, but that was the impetus for the international regime, which is the International Ship and Port Security Code, as well as regimes that now have been implemented as far down as individual port authorities. And, I am not talking about just regimes that are required by the law. I am talking about they understand that security is now part of their business product. So, I think in that regard, there are clear measures.

Really, an intangible, probably, from here to see, but as the Captain of Port, I can tell you, there was no awareness or recognition that security really was part of the product in the port. We had gotten the message across with regard to safety and environment, but now they get it. It is part of their business, as well. So, I think there is a metric there.

And certainly with regard to awareness and capability, we have built the capabilities federally, locally, internationally, all of which, I think, are clear evidence that we have been effective in terms of enhancement.

I am with you. I think we need to do more. I think we can never rest on our laurels. I am concerned about emerging threats like cyber. We need to develop some metrics there.

Chairman CARPER. We will come back. We will finish first. But, how are we doing? What are we doing well? What metrics are we doing? How do they demonstrate where they are doing better? But, I want to come back and see what is on this “to do” list for us. Kevin.

Mr. MCALEENAN. Mr. Chairman, I will touch on five areas. Broadly, our ability to identify and mitigate risk is the metric we seek to measure ourselves on.

First, on the data front, as Ellen alluded to, we are getting advance information on all cargo shipments destined for the United States—manifest information, entry information, an Importer Security Filing, which is another 12 data elements that are critical.

In terms of targeting and assessing that risk, category two, we are analyzing all of it with our automated targeting system, which we think is a very sophisticated capability that is constantly and iteratively approved, and we are currently working on responding to the GAO’s ideas on identifying the effectiveness of those targets with more granularity.

Three, examining at the earliest possible point in the cycle. Currently, 85 percent of shipments that we identify as potentially high-risk are examined before they are laden onto vessels destined for the United States. Our examination requests of our CSI foreign partners at our 58 ports are accepted 99 percent of the time, and we think those are very solid metrics. One hundred percent of containers identified as potentially high-risk are examined before they

are let into the United States stream of commerce. So, 85 percent prior to lading and the rest of the 15 percent before they are allowed to enter the United States on arrival.

Securing the supply chain, category four. Over 50 percent of all cargo containers by value are part of our C-TPAT partnership with our 10,750 partners. We have increased the security of the supply chain through that partnership. We are also mutually recognizing other countries' systems, including the European Union and six other agreements, to ensure broader visibility globally, as Ellen alluded to, the international partnerships.

And, five, our efforts to address the highest consequence threats. Rad/nuc, we are scanning 99.8 percent of all arriving containerized cargo through—

Chairman CARPER. Say that again. What percent?

Mr. MCALEENAN. Ninety-nine-point-eight percent, so just about everything arriving into seaport is scanned through a radiation portal monitor, sophisticated, sensitive technology for identifying radiological and nuclear materials.

The other part of this coin, sir, the facilitation piece that you referenced, the vast majority of cargo arriving in the United States is released before it even touches the dock. Our C-TPAT partners are getting fewer exams because they have secured their supply chains. We have established mobile technology options for agriculture specialists to clear shipments right there on the dock instead of waiting hours and having those bananas sit in Wilmington. The U.S. Chamber of Commerce and 71 others just wrote to the Secretary this week in an open letter saying that this regime is working well and that the facilitation piece, in particular, we have achieved through this layered risk approach.

So, those are the metrics we look at. I am happy to elaborate on any specifics.

Chairman CARPER. All right. Fine. Mr. Kamoie.

Mr. KAMOIE. Mr. Chairman, I think while you were out, what we agreed is that in the Port Security Grant Program, that we have measures, we have made progress, but that we agree we can continue to make progress.

On the programmatic side of the effectiveness measures, we look very carefully at the six priorities of the grant program: Enhancing maritime domain awareness; enhancing improvised explosive device detection; chemical, biological, radiological, nuclear, and explosive prevention, protection, response, and recovery capabilities; enhancing cybersecurity capabilities; maritime security risk mitigation projects; planning training exercises; and the Transportation Worker Identification Credential implementation.

Right now, we have a measure that we are looking at building new capabilities across those six areas and sustaining existing capabilities. But, again, that measure can be better.

On the administrative management side, we have made progress in measuring our ability to effectively and efficiently release the funding, monitor programmatic use of these funds, monitor grantee financial management of the funds, monitor the closing of awards and grantee draw-down. We are making progress, Mr. Chairman, and we have an opportunity to make even more.

Chairman CARPER. Good. Thanks. Mr. Sadler.

Mr. SADLER. Yes, sir. For us, I think it is about getting good, quality information and data for us to make the right decisions on when we issue a card. It is about continuing to get that information after we issue the card so we can monitor the individual to ensure that they have not done something as to disqualifying, whether it is on a Terrorism Watch List or through some type of criminal issue.

I think the other thing that is going to make us better is installing readers. We believe that the Coast Guard, who we are very close partners with, as we are with everyone else on the panel, made the right decision to take a risk-based approach and put readers where they need to be and we think that is going to be a major improvement for our program, considering it is a biometric credential.

And I think the last thing that we have to do is share information, which we do on a daily basis. So, we need good quality information to make good decisions with. We need the information to keep on coming, so we can continue to make good decisions after we issue the credential. We need to install readers. And, we need to continue to share information, which we do on a daily basis with our partners.

Chairman CARPER. Mr. Caldwell.

Mr. CALDWELL. Thank you very much. The most difficult question is how do you measure security and risk, and I think we have looked at that quite a bit across these programs. One of the better measurement programs that we have found is a Coast Guard program called the Maritime Security Risk Analysis Model. They can actually, at the facility level, try to measure the risk based on vulnerabilities and threats and various scenarios and like that.

The Coast Guard also took a step trying to develop a more sophisticated measure of how much Coast Guard programs actually reduced risk in the port environment—their estimated percentage reduction of maritime security risk subject to Coast Guard influence. We were critical of this, because in the end, it was subject matter experts in the Coast Guard sitting down and thinking about what those reduction measures are and then putting a single point of percentage on that.

We had a couple of criticisms in terms of ways they could try to make that better. When there is so much judgment, you want to give a range instead of a point estimate. But, I do not want to be too critical of the Coast Guard in the sense that they certainly were trying to think larger about their suite of programs and to what extent they reduce risk.

They are looking at whether they want to keep that measure or not. It was a measure they were using within the Coast Guard. But they actually were not really using it to direct resources or conduct operations. So, if you have a performance measure but you are not really using it to monitor things or prioritize resources, you have to question whether it is a useful metric in the end. Thank you.

Chairman CARPER. OK. Some of you began to answer the second part of my question, but I want to take another shot at it. My staff and my colleagues oftentimes hear me say these words. The road to improvement is always under construction, and that is true here, as well. I just want to, in terms of, again, thinking of metrics, but

thinking of areas, not where we are making progress but areas maybe where we have not made nearly enough—there has been some allusion to this, but some areas where we have not made nearly enough, and we can actually measure that we have not made nearly enough—are there any of those—think about it out loud—who can help enable us to make the progress that is needed? Us, the Legislative Branch? This Committee? The President in his budget? Who needs to help out?

Ellen, do you want to go first?

Ms. MCCLAIN. Yes, Mr. Chairman. I think that, just to sort of set the scene here, we certainly need an approach that is flexible, innovative, so that we can take on the adaptive adversary, and we need something that—an approach that is risk-based so that we can make the most cost effective use of our resources. That said, we recognize that we do not want to have negative impacts on global trade.

So, we are looking in the near term to specific improvements in the area of the targeting algorithms, reducing the false alarms, working with our partners at some of the CSI ports to increase the percentage of scanning that is undertaken. We are looking at, and I think this is a key point that I hope does not get lost in today's discussion, across all pathways, focusing on a single pathway does not necessarily reduce overall risk. So, as we go forward, we need to consider improving security across all transportation pathways.

And, last, I would note that we are continuing the dialogue with stakeholders to see what additional or expanded roles they might take in improving the security of our ports.

Chairman CARPER. OK. Thanks. Admiral.

Admiral THOMAS. I think there are a couple areas that I would be concerned about. The first is complacency. As we get further from 9/11, I think the sense of urgency decreases. And so from the Congress on down to the security guard at a facility, we have to make sure we maintain the sense of urgency with regard to port security, because the threat is adaptive, and as good as the physical security systems that we have in place are, there are emerging threats like cyber that we have not yet addressed. We have begun to address them. I believe the Coast Guard has the authorities that we need to do that and we are working on what the resources might be, so you may hear about that.

The other area that would be of concern is the real high-end threat that needs to be intercepted as far offshore as possible. We need to maintain the ability to get out there and do something about some identified threat that is bound for our shores, and that is a real challenge because it requires ships and helicopters and people that are not only capable of getting there, but are present at the time when you need them.

So, those two things are areas where we need to make sure that we continue to build our capability and to build our plans for action.

Chairman CARPER. Great. Thank you. Kevin.

Mr. MCALEENAN. Mr. Chairman, I would echo a couple of the comments that Ms. McClain made. On the targeting side, there is always an opportunity to improve our analytics and our capabilities to assess risk and we are pursuing that aggressively. We have a

good system for taking in current intelligence, manipulating the data elements against it, and identifying risk, but we want to continue to get better. So, that is an area, and we do get Congressional support to continue to improve in that area.

With the radiation portal monitors, we need to be able to dial the algorithm so they are very sensitive for the threat materials we are worried about, but they reduce the naturally occurring radiological material alarms that we face on normal commodities, like bananas, for instance, and granite, and other things that do hit on our radiation portal monitors. We do not want to waste time on those alarms. We want to focus on what could potentially be dangerous material.

I think there are continued opportunities globally. We are currently working with partners on broadening the scope of CSI, security first, but also looking at other threats to the goal of supply chain—contraband, commercial fraud that can support criminal activity, and so forth. Enhancing global supply chain security standards—we did that after 9/11 with the World Customs Organization and the same framework of standards. There are always opportunities to take that to the next level and to build capacity with those governments and customs services that are willing to step forward but do not have the internal capacity or funding.

And then, of course, the private sector, continued opportunities there, not only on the supply chain side with C-TPAT, but looking at whether, from a terminal operator perspective, there might be a return on investment to do greater security work prior to lading from a private sector perspective that we could then share and benefit in. So, we are pursuing all of these angles as the Secretary noted in his letter.

Chairman CARPER. Those are great points. I really appreciate your responses. I will come back and we will ask the same question of the last three witnesses, and I will be right back, Tom.

Senator COBURN. Do you want them to answer those, or do you want to—

Chairman CARPER. No, I will do that when I come back.

Senator COBURN. [Presiding.] OK. Thank you.

Let us talk about the 100 percent mandate and the fact that we are at 2 to 4 percent. I think those numbers are right. Please correct me if I am wrong. And, GAO, I would love for you to get in on this. There is no question, the 9/11 Commission said, for port security, we need 100 percent screening. And what we hear is, that is not practical.

So, the question is somewhere between 2 to 4 percent and 100 percent, where do we need to be? How do we need to decide where we need to be? How do we become more effective in terms of container inspection? Admiral. Kevin.

Mr. MCALEENAN. Senator, I will start, and I am sure colleagues will want to chime in. On the 100 percent mandate, I think the key question for us is not the percentage itself, but are we inspecting the right percentage. Are we inspecting and identifying those containers that are high-risk and mitigating that threat at the earliest possible point?

While you had to step out to vote, Senator, we talked about some of the metrics that we are following and whether we are accom-

plishing that and I would just like to reiterate one of those elements for you, sir. On those containers that we identify as potentially high-risk through our Automated Targeting System (ATS), we are currently examining, with our foreign partners under the Container Security Initiative, 85 percent of those containers before they are ever laden on a vessel destined for the United States. So, within that—

Senator COBURN. So, that is 15 percent that are not getting inspected.

Mr. MCALEENAN. They are getting inspected fully at the first port of arrival in the United States. So, we are checking them before they enter the stream of commerce to the United States, and we are getting 85 percent of them before they are even on a ship destined for the United States.

Senator COBURN. OK. But, if that 15 percent, one of them has a nuclear weapon in it, it is a little late, is it not?

Mr. MCALEENAN. Yes, but that is not the only layer that we have in place prior to lading.

Senator COBURN. I understand, but when we think about this, you are saying 85 percent of those deemed high-risk. So, what is our goal to get to 100 percent of those deemed high-risk?

Mr. MCALEENAN. So, our goal there, sir, is to increasingly target with the right foreign ports—how we can encourage them to examine anything that we think is high-risk before lading. So, we have 58 CSI ports covering over 80 percent of cargo destined for the United States. We think we have placed those CSI locations in the right places. We are currently, though, assessing how the threats have changed. Are there certain strategically important ports that we can add capability? Can we work with additional countries to encourage them to take some measures before lading?

Also, just mentioning as you came in, sir, working with terminal operators in the private sector. Is there a way that we can encourage terminal operators to increase the overall inspection if they think there is a return on investment, working with their customers to sell a security benefit that we could then benefit from and share in the information, also.

Senator COBURN. All right. Admiral, any comments on that?

Admiral THOMAS. The container inspection world really does belong to Customs and Border Protection, although I can certainly attest to the impracticality of looking at every container as it comes through our yards. I have seen the targeting that we do jointly on cargo and the automated processes really are very effective and very adaptable. So, if there is a new intelligence stream that comes in, we can very quickly, or CBP can very quickly change their targeting and identify cargo that might be associated with a newly identified threat.

Senator COBURN. All right. So, here is the question, as a common sense Okie, we are saying it is not capable to do 100 percent screening. Where is the study that says, here is what this will cost and here is what this will slow down commerce? Has that been done?

Mr. MCALEENAN. A number of studies in that regard have been done, and I would offer the GAO might want to comment, as well. We have done a study and provided several papers to Congress es-

timating up to \$16 billion in costs. The European Union has done a study. The private sector has done several studies.

The challenge is, sir, there are 800 or so initial ports of lading for containerized cargo destined for the United States, an average of three to five lanes per port, an average of five million to implement this kind of system prior to lading in each lane, and that scope just makes it very challenging to get to that level. There are a lot of questions on who pays, who is responsible, how it is monitored, and so forth.

Senator COBURN. So, if you take the RAND study, even though it is dated now, and say, if one sneaks in and you have the tragedy that they spoke about at the Port of Los Angeles, estimating a trillion-dollar effect on our GDP, \$16 billion does not seem that great. So, where do we go, GAO?

Mr. CALDWELL. Senator, thank you. We have done several studies on it. As far as the type of study you are asking for, the only place I have seen it is in a recommendation we have made. I think that CBP and the Department would have been better off if, at that point, they just said, OK, we will do the required feasibility study. This would have included a cost-benefit analysis. CBP could have done it then and tried to put this thing to bed, or at least show what those tradeoffs are. Certainly, there have been multiple small pieces of analysis, so I feel bad. Because I think the Department, in all the little pieces of analysis they have done since then, have almost gotten there.

I would also like to stop to talk about one popular myth. The 9/11 Commission Report never called for the 100 percent scanning of maritime cargo.

Senator COBURN. What did they call for?

Mr. CALDWELL. They called for 100 percent scanning of air cargo. The report said almost nothing about ports and maritime security.

Senator COBURN. OK. That is great to know.

Mr. CALDWELL. But, moving on, we do think the challenges to 100 percent scanning are likely insurmountable. The SAFE Port Act left a lot of things undefined, and I think through the pilots, CBP tried to understand what those undefined things would actually be in terms of cost, and who does it.

But, there is also a concern that it would create a false sense of security. You could scan a container. If it is done within a customs regime that we trust, a port terminal that we trust, then we have some confidence that after the container is scanned and gets on that ship, it is going to be monitored. But, a lot of times, we will not have that case. In a lot of the cases, because of how ports are laid out, scanning is done offsite. If that truck with the container has to drive three to five miles to an from the scanner a lot can happen in that distance.

The former Coast Guard Commandant Thad Allen said he thought it was more likely that a weapon of mass destruction would come in to the United States not through a highly regulated regime like containers, but into the United States in some small vessel coming in or snuck in some other way.

I also agree that intelligence will, in the end, be the key, to revealing any weapons of mass destruction (WMD) that terrorists are trying to smuggle in. I am not sure ATS by itself would catch that.

They have looked at millions and millions of containers and used the risk-based analysis. Yet they are still finding contraband, but, it is not like when they find drugs in these containers that there is a one-to-one match between, we had rated that containers as high-risk. There are many cases where they find illegal stuff in containers that had gotten through their ATS system, drugs or other contraband.

Our approach at GAO has been to look at the programs that we have. We still would have liked to have seen DHS and CBP do that feasibility analysis of 100 percent scanning. At this point, we have closed that recommendation as not implemented. I think that is water under the bridge. We would like to see CBP doing better with the programs we have, recognizing that we are not going to have a perfect system. One improvement would be optimizing your targeting system, which means that you are monitoring it on a regular basis. You are testing it to see how it is doing. Another improvement is having the best CSI footprint you can in terms of some of the CSI program focusing on high-risk ports. If not, maybe CBP should pack up and shake hands with those partners. Those partners will keep helping us, but CBP could move some of those CSI operations to other ports.

Senator COBURN. Do you have specific recommendations on ports from the GAO?

Mr. CALDWELL. Yes, we do. We have a recommendation that CBP use the port risk model they had used in 2009 to initially plan the 100 percent scanning, or a similar type model to figure out what ports they should actually be in. We tried to reproduce that type of analysis and found that about 12 of the CSI ports CBP was in were low-risk ports. More than half of the CSI ports were in high-risk ports. We recognize that there are some ports that are not going to let us in. I mean, you have some nasty players out there that are not going to let a joint U.S. program into their ports—I am not at liberty to disclose details of individual ports, but there is movement in terms of additional CSI ports, both opening and closing.

Senator COBURN. OK. Let us go back to grants and the tiered port system for a minute. If we are not doing analysis on progress, do we reevaluate the ports in terms of tiers? Here is tier one, tier two, tier three, tier four. Is that done routinely? Yearly? Biannually? How often do we reanalyze high-risk ports, one? No. 2 is, without the metrics, but they are getting better, how do we take what we have improved and measure it to show a decreased risk for a tier one port so that the dollars that you have can go to where the risks are the greatest?

Mr. KAMOIE. Thanks for the question, Senator. We reassess the risk of the Nation's ports every year, and we use the risk formula that incorporates the most recent data we have available on threat, vulnerability, and consequence. And, there have been times where changes in that risk data have resulted in the changes in the grouping of ports. For example, last year, in fiscal year 2013, there are eight tier one ports. San Diego had a change in its relative risk formula, because these are relative to one another, and so this year, it is not a tier one port. So, we are making those adjustments. We work very closely with the Department's Intelligence and Anal-

ysis unit to populate the risk formula with the most recent data. So, yes, we are looking at that continually.

Your second question, as to what the measurement and, really, what I would consider to be buying down of that risk and the vulnerability, I agree, we have some progress to make there in terms of agreement on measurements and metrics to show that progress, and show it in a way, and when the Chairman comes back, his question was about how can the Congress help, and here, I think, my ask of the Chairman and you, Senator, is that we have a continued dialogue about the types of data that would enable you to have more confidence and the American people have more confidence that we are making that progress and that we are being effective stewards of the taxpayer dollars. I agree with you that we certainly have made progress and we have plenty of good examples, but we would like to continue to work with you to get at the data and the measurement that would show that in a more compelling way.

Senator COBURN. Each port has a Port Security Plan, right?

Mr. KAMOIE. Yes.

Senator COBURN. All right. Has Homeland Security done an analysis of what the total cost would be to bring it up, on a cost-effective benefit, how much total for all the tier one ports would we need to spend to bring them to where they need to be? Do we have that? Do we know that?

Mr. KAMOIE. I am not aware of that analysis—

Senator COBURN. Well, that is—

Mr. KAMOIE. We will have to followup.

Senator COBURN. That is an important question, because if you do not know what they need, we will never get there, and—

Mr. KAMOIE. Well, so, I mean, we certainly, at the Captain of the Port level—

Senator COBURN. I know you know where the weaknesses are, and I know that is where the grant money is going, but I am saying, in the big picture—

Mr. KAMOIE. Sure.

Senator COBURN [continuing]. If we are going to spend \$100 million this year on Port Security Grants, and the total bill for bringing our tier one ports is \$2.5 billion, we are 12½ years from bringing them, and by that time, you are going to have replacement needs. So, the question is, do we not think it is important to really know by port, here is the total cost to get us where we want you, and which one, out of those top eight ports, which one has the greatest vulnerability basis and should we not be spending maybe \$70 million at one port and \$30 million at the other eight on the basis of what the total need is to bring them to that level where we feel confident?

Mr. KAMOIE. Sure. We will absolutely take a close look at that. We have moved the entire suite of grant programs toward performance measurement against the core capabilities that are in the National Preparedness Goal, following up, implementing Presidential Policy Directive 8 on National Preparedness. We continue to find the performance measures for those. But, we are through the threat hazard identification and risk assessment process. We are asking grantees to do a lot of what you are talking about in terms

of identifying capabilities and then using the investments to close the capability gaps.

So, we are moving in that direction, but I am not aware of a single analysis where we have put a price tag on, by port, what it would take to close the gap in every port against one level, but we will certainly take a look at that.

Senator COBURN. Well, I just think that would be really important to know, because you are going to have limited funds—

Mr. KAMOIE. Yes.

Senator COBURN [continuing]. From here on out. It is not going to change. And, sending the dollars where this is all risk-based, right?

Mr. KAMOIE. Yes.

Senator COBURN. Sending the dollars where the greatest risk is should be our priority. So, I would just recommend you look at that. I do not know if the GAO has any comments on that or not—

Mr. KAMOIE. Senator, if I might, we will take a close look at that. I think the threat hazard identification risk assessment process and the Area Maritime Security Working Groups at the port level, I think they are getting at a lot of that. But, I agree with you. We could make even more progress.

Admiral THOMAS. If I could, on two of your points: The first had to do with how do you account for risk bought down with previous grant money in determining the risk ranking for the next—we actually do that as part of the Coast Guard's Maritime Security Risk Assessment Model that GAO mentioned. If we have invested in a system that reduces the vulnerability or mitigates the consequences of an attack on a facility, it gets reflected in our model. That data is part of the risk formula that DHS then uses to determine the tiers for the next year. So, it is in there.

The other piece that you asked about is have we defined what a secure port is and when will we know that we get there. That is an interesting question. What I can tell you, though, as a Captain of Port, is I watched the initial focus be on securing individual facilities, so, let us make sure we have fences and cameras and guards and Radiation Portal Monitors (RPMs) and get facilities.

And then I saw it evolve to, well, we need to really secure this port as a system, as well, so how do we link these fences together? So, we invested in things like communications systems that will allow everyone—and surveillance systems that were focused on the common infrastructure, not on the private sector infrastructure.

And, we said, well, that is good, but have we been able to address what we are going to do if we get attacked and we need to recover? So, we invested in trade resumption plans.

And so it has been a natural evolution. I believe we are still in that evolution because we have emerging threats such as cyber. I think the next round of grants is putting money toward cyber vulnerability assessments so that we can then understand what it is going to take to secure the cyber infrastructure of the maritime—I do not know that we will ever be able to say we are there, but I do see a very logical progress on how we focused our planning and our investment.

Senator COBURN. We have a diagnostic system for cyber within Homeland Security. Is the TWIC system applicable to that system?

Mr. SADLER. Let me take that one, sir.

Senator COBURN. Yes.

Mr. SADLER. So, right now, the way the TWIC system works is that the contractor provides the enrollment equipment and then they connect to a system that eventually gets back to TSA, and that system, whether it is on the enrollment side, the data center side, up to the TSA side, is built to Federal standards. They have to go through a certification and accreditation. They go through auditing. They go through testing. So, it is not monitored within the DHS system. It is monitored through the TSA operations center. So, everything from the contractor's data center practices—

Senator COBURN. You have answered my question. Got it. Mr. Sadler. OK. Thank you.

Chairman CARPER. [Presiding.] I would like to come back and ask Mr. Kamoie, Mr. Sadler, and Mr. Caldwell to answer my earlier question, please.

Mr. KAMOIE. Absolutely, Mr. Chairman.

Chairman CARPER. And then, just so you will know, the next question I am going to ask of all of you is what do we need to do? What is our "to do" list on this Committee and in the Congress to make sure we continue to make progress? Thank you.

Mr. KAMOIE. Absolutely, Mr. Chairman.

Chairman CARPER. All right. Mr. Kamoie.

Mr. KAMOIE. My ask of you and the Committee is for continued dialogue—and I shared this with Ranking Member Coburn before he stepped out—a continued dialogue about the types of data and the types of measures that would give you the confidence, give the American people the confidence that we are investing the grant dollars in a way that is most efficient and most effective and that we are all good stewards of these resources.

I agree with Admiral Thomas. The threat is evolving. So, too, have our measurement of where we are headed next. So, I would appreciate a continued dialogue with you about how we define the measures of success that will give you the confidence that we are all looking for.

Chairman CARPER. OK. Thanks.

Mr. Sadler, something for our "to do" list to help continue to make progress.

Mr. SADLER. I think it is just continued support and helping us get, from TSA's point of view, the readers out, and the Coast Guard's point of view, understanding that the Coast Guard is promulgating the rule, but there were a lot of things that had to happen before they got to the point where they can do that. So, when I say we need the readers, we need the readers. That is not in any way insinuating that there is some delay on the rules side. There was a lot of work that went into getting to this point. So, we would ask for the continued support so we could put readers in place, we could buy down some risk, we can use the full capabilities of the card.

And, I think, to the Admiral's point before, it is critical that we maintain mission focus. It is also critical that we make risk-based decisions so we protect the right areas. And then for our look at

it, it is data quality, it is identity verification, it is reduction in fraud, it is ensuring that the right people get the card and the right people keep the card after it has first been issued.

Chairman CARPER. All right. Thank you. Mr. Caldwell.

Mr. CALDWELL. So, I am going to provide a combo answer because I am still trying to answer the question you asked before, I have three things, two for the agencies to do and one for the Committee to do.

First off is for agencies keeping the programs flexible. The Coast Guard is trying to make their infrastructure security patrols less predictable so you improve the level of deterrence. I like what I see at CBP as well when they are doing what they call their quayside or dockside scanning. In such cases a ship will come in and CBP will target that ship. It will not be based on whether the containers are high-risk or not. CBP will be scanning every seventh one or tenth one container coming off. They could be a little more flexible in CSI and the footprint they have and think about whether they need to shift that footprint a little bit to cover different countries and ports, if possible.

I think cyber is the growing area. That is an area where DHS and the Coast Guard have been monitoring the situation, and they are talking about taking action. We will have a report we are issuing tomorrow for the Senate Commerce Committee that will have a lot more detail on that.

And then something for this Committee, and I think it is starting to show up on the radar of the agencies. We do have to sustain current equipment. You have vessels and you have scanners and you have aircraft that are pretty important in this security regime. This is true particularly in terms of some of the interdiction and the deterrence missions and just the daily things like scanning containers. Some of these assets are reaching the end of their life. I know that CBP is trying to extend the range of their scanners from, say, 10 years to 13 years. But, at some point, you are going to have to replace them. Now that you have built this security regime and all the things that go with it; sustainability will translate into resource requirements just to keep what we have.

Chairman CARPER. OK. The last three witnesses have pretty much sort of gotten to my last question, which was, what is our "to do" list? And, I do not know that, Ms. McClain, you and Admiral Thomas and Mr. McAleenan had a chance to do that. Our "to do" list—do you—

Ms. McCLAIN. Chairman, I think I just echo some of the points that were made earlier and emphasize that in moving forward, anything we do needs to take into consideration that DHS confronts a multitude of threats. And so to be cost effective and efficient, we need to always bear that in mind.

I think the second point we made earlier is that, big picture, we must focus security across all pathways, to buy down risk, we do not want to encourage sort of a balloon effect where we put all our security assets over here and the agile adversary just circumvents that. So, the picture has to be across all pathways.

And then echoing Mr. Caldwell's point about support to address the aging infrastructure and funding DHS in accordance with the President's budget. Thank you.

Chairman CARPER. OK. Thanks.

Admiral Thomas, anything you have that we should be doing on the legislative side.

Admiral THOMAS. Thank you, Chairman. I do not have much to add to what has been said. There may be some very specific authorities and capabilities that we identify as we continue to analyze the threat in the ports, but I think we have the right access through the staffs to get that information to you.

I would say that this type of oversight and continued focus by this Committee on this issue is really important to stave off that complacency that I am concerned about, so we do appreciate that.

Chairman CARPER. Thank you.

Mr. MCALEENAN. Four quick things, echoing several things that Mr. Caldwell mentioned. We need continued support for the key programs we have discussed today, the Automated Targeting System, CSI, and we are actively working on the recommendations that Mr. Caldwell mentioned.

Recapitalization and sustainment of our critical technology, radiation detection equipment and Non-Intrusive Inspections, along with the Domestic Nuclear Detection Office, we will be working with your team on those plans.

Three, what you articulated at the beginning, Mr. Chairman, understanding the critical economic, expeditious, and facilitated movement of cargo aspect of our mission. That continues to be critical and needs to be understood.

And then, four, working with the Secretary and the Department on an agreed path forward on scanning, keeping us honest on the good faith efforts you identified and we discussed today, but also working together on the best framework for the future.

Chairman CARPER. Good. Thanks.

I think Dr. Coburn, when I was out voting, asked a question dealing with fiduciary agents, and I just want to come back and—he asked part of my question. I just wanted to come back and say the second half of the question. Maybe you all could take a shot at it. I need to be someplace else, in 8 minutes, so whoever would—Brian, I am going to ask you to take the shot at this one—

Mr. KAMOIE. Absolutely—

Chairman CARPER. Rather than ending the use of fiduciary agents for all ports, why not let ports decide for themselves if they would like to use one?

Mr. KAMOIE. We have considered that proposal and do not think it is in the best interests of the program if some are using fiduciary agents and others not. I mean, the benefit we have derived by moving away from the fiduciary agent model is, as the appropriations have gone down and our capabilities internally have grown in terms of program oversight, management, and monitoring, we have gotten a pretty good window into the project level data and the approach grantees are taking. And, we lost some of that visibility, as you might expect. There was a variety of performance, varying levels of performance across the fiduciary agent model.

And then the other thing is with the management and administration fee, the fiduciary agents had access to 3 to 5 percent of the funds. We think those funds are better invested in actual security projects.

So, I know that there is a range of opinions in the port community about the fiduciary agent model, but we have decided that the best thing for the most effective and efficient management of the program is to bring that management in-house and not use the fiduciary agent model.

Chairman CARPER. OK. Thanks.

And, this last question would be for Ms. McClain, Admiral Thomas, and Mr. McAleenan. Really short answers, if you would. The first question is, what effect has increased security along our land borders had on maritime border security? Ellen, if you could just take 30 seconds.

Ms. McCLAIN. Yes, Mr. Chairman. Two quick points. I think the Trusted Trader Programs that we developed in the land border context informed how we deal with those programs in the maritime context.

And, second, I think it pointed out to us, and I will quickly go back to South Florida in the 1980s, how you need a risk-based approach across all pathways to secure any single pathway. Thank you.

Chairman CARPER. Thank you. Admiral.

Admiral THOMAS. Well, somewhat outside of the realm of port security, but certainly, we have seen the balloon effect on particularly the Southern part of the West Coast and also in the Caribbean. As we secure our land borders for illegal drugs and contraband and other illegal activities, they have taken to the water, and so we have adjusted our forces and that is really the impact that we have seen there.

Chairman CARPER. OK. Thank you.

Mr. McALEENAN. I agree with the Admiral. We have not seen a significant impact in terms of changes in the threat within commercial flows. We have seen the effect of security between ports of entry push activity out into the littorals on the West Coast as well as up through Puerto Rico.

Chairman CARPER. OK. There is a second half to that question, but I do not have time to ask it. You may not have time to answer it.

I am just going to wrap it up here. I am really glad that Dr. Coburn encouraged us to have this hearing. This is timely. There is a fair amount of progress to be reported on and there is still plenty of work to do. I am encouraged that the sense of team is at play, and that certainly helps, and we are part of that team. But, thank you all for your preparation today, for coming and helping to make this a very great hearing.

It is clear to me that one of the most important take-aways from today's hearing is that it is critically important that we strike the right balance. It is not an easy thing to do. It is easy to say, but it is hard to do, strike the right balance between security, trying to make sure we do not unduly impede the flow of transportation and trade. As we all know, what did we say, 95 percent of our trade moves on the water, but the port surge is vital to our Nation's well-being and they are a conduit for a lot.

With that, I am going to call a halt to this. Some of my colleagues are going to have some questions to ask, and we may have some ourselves, so the hearing record will remain open for 15 days.

That is until June 19 at 5 p.m., for the submission of statements and questions for the record.

With that, I would say to our Republican staff and our Democrat staff and all my colleagues, thank you very much for your help in this, and to each of you for joining us today. I think one of you, it was maybe you, Admiral, said oversight is a good thing, and we hear that a lot, so we will not disappoint you. Thanks so much.

With that, we are adjourned. Thank you.

[Whereupon, at 12:27 p.m., the Committee was adjourned.]

# A P P E N D I X

---

**Opening Statement of Chairman Thomas R. Carper  
“Evaluating Port Security: Progress Made and Challenges Ahead”  
June 4, 2014**

*As prepared for delivery:*

We have called this hearing to take a look at the current state of port security in the United States and find out if we are heading in the right direction. I hope we can also focus on the work that needs to be done over the next few years to ensure that our port security efforts maintain the proper balance between security, safety, and trade facilitation.

This is important because our focus as a Congress cannot solely be on security, but also on maintaining and enhancing our economic competitiveness. Port security is no easy job.

It involves the maritime security provided by the U.S. Coast Guard when its men and women patrol our coasts and waterways. It involves the physical security of port facilities, like our ferry terminal in Lewes, Delaware, or an energy refinery along the Gulf of Mexico or Delaware City, Delaware, that is safeguarded by state and local authorities. And it involves the cargo security provided by U.S. Customs and Border Protection, which screens cargo to prevent dangerous goods from entering the United States, while also facilitating the flow of trade and transportation.

That last part is a particularly important piece. Even as we build and maintain strong layers of port security, we need to take care to not impede transportation and commerce.

Our ports and waterways are the lifeblood of our economy. More than 95 percent of all U.S. trade is handled by our seaports. These ports account for over 30 percent of U.S. Gross Domestic Product. That's more than five trillion dollars in trade each year.

As the former Governor of Delaware and someone who was ultimately responsible for running a major port, I have a good appreciation of the important role they play in our economy. The Port of Wilmington, located along the Delaware River in the northern part of my state, is the number one seaport in North America for the importation of fresh fruit, bananas, and juice concentrate.

The Port of Wilmington isn't just important for the State of Delaware, where it serves as a key economic engine in New Castle County; it's a key port for the entire east coast of the United States. So protecting our ports, and safeguarding our economic lifeblood, is a responsibility I take very seriously.

As the Government Accountability Office and other experts have noted, U.S. port security has come a long way. Shortly after 9/11, the Maritime Transportation Security Act of 2002 became law and empowered the Coast Guard with new authorities to ensure commercial vessels and port facilities meet minimum security standards.

A few years later, the SAFE Port Act of 2006 authorized key cargo and supply chain security programs enforced by U.S. Customs and Border Protection. Since that time, these port and cargo security programs have matured and taken root. Not only that, many of our international trading

partners, and international trade and security organizations, have created similar security programs, emulating the Department of Homeland Security's good work. But we shouldn't – and we can't – stop here.

I want to use this hearing as an opportunity to explore how the threat to ports has evolved and what the next steps for DHS should be. I also don't want to imply that there is no room for improvement. I frequently say, I know everything I do, I can do better.

In a recent letter to Congress, DHS Secretary Jeh Johnson indicated that he believed the 100 percent scanning mandate for inbound cargo shipping containers was impractical, and not the best use of taxpayer resources. If that is the case, we must look for a better way to address security risks while preserving the necessary speed of moving containers through the ports.

So I welcome the Secretary's pledge to make a good faith effort to improve the Department's capabilities, without getting in the way of the legitimate flow of trade. I look forward to discussing this issue with some of our witnesses.

I also look forward to hearing how the Department of Homeland Security plans to address emerging threats, how it can make programs more effective and efficient, and how the agencies represented here today can work with international organizations and foreign partners to raise the global standard for port security.

As you can see from our lineup of witnesses, port security is a team sport. It's a perfect example of why bringing all of these agencies together into the Department of Homeland Security was the right thing to do. The components present here today work seamlessly with one another to develop and implement the Department's layered, risk-based strategy for port security.

From the Coast Guard to Customs and Border Protection, the Transportation Security Administration, the Federal Emergency Management Administration, and DHS's Office of Policy – each plays a critical role, and all must work together.

I am also glad to have the Government Accountability Office with us today, because it has done a considerable amount of work in this area. I thank you all for being here today, and I look forward to your testimony.”

###

**Hearing: "Evaluating Port Security: Progress Made and Challenges Ahead"**

Opening Statement of Dr. Tom A. Coburn, Ranking Member

Thank you, Mr. Chairman.

First, I would like to welcome all of you. This is an interesting area for us to be talking about. Sitting on the Intelligence Committee, our threats are greater, not less, in terms of risk and getting it right is important.

One of the commitments I made to Congresswoman Janice Hahn from Los Angeles, CA, she has the Port of L.A./Long Beach, which is our largest, busiest and probably most vulnerable port. We are having this hearing and doing the oversight that's necessary to try to improve the security at our ports. So, Mr. Chairman, I'd like unanimous consent to put her testimony in the record. The Congresswomen wanted to participate in this hearing but the House is out this week, and so I'd ask unanimous consent to have her testimony included in the record.

I'd also note that the House has passed legislation that the Congresswoman authored called the GAPS Act. What I hope we do today is find out where our weaknesses are and what we need to improve. As Senator Carper mentioned, the 100 percent scanning mandate may not be viable, but we need to have a better approach than 2 percent to 4 percent scanning that we're seeing today.

We know that a successful attack on one of our ports would be devastating; the RAND Corporation gave an example that would have a trillion dollar effect on our economy. That is a high possibility. We cannot stop every attack that's going to come to this country, but we can certainly make it much more difficult and markedly decrease the likelihood. Everybody knows the history of how we came together after 9/11. We created the Port Security Grant Program; we mandated 100 percent cargo screening; we also created the TWIC card, which has had some significant difficulties and is still not implemented.

So my goal for this hearing is to review all the initiatives that were initially set out, assess whether or not they're working and determine if our ports are as secure from a potential terrorist attack as we can make them feasibly and economically.

I would say we've spent \$2.9 billion on the Port Security Grant Program with no metrics to measure whether or not we have actually improved our security. There's no metrics, so we don't know. We've spent \$2.1 billion on CBP cargo programs to meet a scanning mandate that we are told will never be met. So there's \$5 billion we've spent we have no assessment of what we've improved with that money. The TWIC program was intended to create an I.D. card for transportation workers to enter secure areas, including the ports. In general, I hope this hearing will help us to know how much improvement we've actually made in securing our ports. I want to thank each of you again for being here.

**THE U.S. SENATE COMMITTEE ON HOMELAND SECURITY  
AND GOVERNMENTAL AFFAIRS  
ON**

**“EVALUATING PORT SECURITY: PROGRESS MADE AND CHALLENGES AHEAD”**

**JUNE 4, 2014**

**JOINT TESTIMONY OF**

**Ellen McClain  
Deputy Assistant Secretary for Transborder Policy  
Department of Homeland Security**

**RDML Paul Thomas  
Assistant Commandant for Prevention Policy  
U.S. Coast Guard**

**Kevin K. McAleenan  
Acting Deputy Commissioner  
U.S. Customs and Border Protection**

**Steve Sadler  
Assistant Administrator, Office of Intelligence & Analysis  
Transportation Security Administration**

**Brian E. Kamoie  
Assistant Administrator for Grant Programs  
Federal Emergency Management Agency**

**INTRODUCTION**

Chairman Carper, Ranking Member Coburn and distinguished Members of the Committee, thank you for the opportunity to appear before you to discuss the Department of Homeland Security’s (DHS) efforts to ensure secure, efficient, and resilient operations at our Nation’s 361 maritime ports and throughout the global maritime transportation system.

The United States is a maritime nation with one of the world’s longest coastlines (measuring more than 95,000 miles), the world’s largest Exclusive Economic Zone, and thousands of miles of internal maritime waterways all enabling a robust exchange of goods, services, and information across our borders. This maritime system supports our way of life and contributes to our national security and economic prosperity. The very nature of trade in our networked world means that a disruption – whether natural, accidental, or malicious – in one part of this system

can have implications thousands of miles away. Beyond loss of life and physical damage, these events can cause considerable economic consequences.

Seven years ago when the SAFE Ports Act was passed, we lacked a fully developed, multi-faceted, and layered approach to mitigating these potential risks and disruptions. The SAFE Port Act, touching as it did on most aspects of the overall maritime architecture, guided DHS' development of the current regime that includes the cargo and vessels that transit the supply chain as well as the ships, facilities, and workers that operate within that system. DHS values the continued dialogue we have had with this Committee over the years as we worked to implement the Act's many provisions. We appreciate the Committee's recognition of a number of notable DHS successes through the codification of initiatives and programs that DHS undertook immediately after the 9/11 terrorist attacks and has been implementing ever since. Representatives from the U.S. Coast Guard, the U.S. Customs and Border Protection (CBP), the Federal Emergency Management Agency (FEMA), and the Transportation Security Administration (TSA) are here to outline the progress we have made in port security since the passage of the SAFE Ports Act, discuss the strategic context and emerging trends and challenges.

## **OVERVIEW**

Following the 9/11 attacks, Congress established a new port security framework—much of which was set in place by the Maritime Transportation Security Act (MTSA). Enacted in November 2002, MTSA was designed, in part, to help protect the nation's ports and waterways from terrorist attacks by requiring a wide range of security improvements. Among the major requirements included in MTSA were (1) conducting vulnerability assessments for port facilities and vessels; (2) developing security plans to mitigate identified risks for the national maritime system, ports, port facilities, and vessels; (3) developing the Transportation Worker Identification Credential (TWIC), a biometric identification card to help restrict access to secure areas to only authorized personnel; and (4) establishing a process to assess foreign ports, from which vessels depart on voyages to the United States. The Department of Homeland Security (DHS)—itself a creation of the new security environment brought on by the 9/11 attacks—administers much of this framework, which also attempts to balance security priorities with the need to facilitate legitimate trade.

The SAFE Port Act, which was enacted in October 2006, was a valuable addition to this port security framework. The Act made a number of adjustments to programs, creating additional programs or lines of effort and altering others. The SAFE Port Act created and codified new programs and initiatives, and amended some of the original provisions of MTSA, including provisions that codified the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT), programs administered by CBP to help reduce threats associated with cargo shipped in containers; set an implementation schedule and fee restrictions for TWIC; and required additional data be made available to CBP for targeting cargo containers for inspection.

## RISK BASED AND LAYERED APPROACH

The Department's maritime and supply chain security doctrine is grounded on a commitment to deploy a multi-layered approach to security, one that is informed by an evolving appreciation of dynamic risks. By deploying multiple, mutually-reinforcing security layers and tools, we are better positioned to identify and intercept external threats before they reach U.S. shores, to reduce vulnerabilities within our maritime critical infrastructure, and to respond to and recover from attacks and incidents should they occur.

DHS's multilayered and risk based security approach extends well beyond our domestic ports and borders. DHS' activities take place at different locations, at different times, and by different organizations based on their jurisdiction, capability, and responsibility to improve security. However, in general, the approach includes five broad elements, to include:

- Understanding the Risk. Assessing and defending against the diversity of radiological and nuclear risks and other relevant risks that may impact the maritime transportation system as well as key vulnerabilities in other pathways.
- Advance Information and Targeting. Obtaining information about cargo, vessels, and relevant individuals early in the process and using advanced targeting techniques to assess risk and build a knowledge-base about the people, companies, facilities, conveyances, and cargo in the supply chain;
- Early Action through Collaboration. Expanding enforcement efforts to points earlier in the supply chain than simply at our borders through collaboration with other Federal agencies, foreign governments, and other stakeholders;
- Domestic Security Regimes. Maintaining robust inspection regimes, including personnel, technology, and access control protocols at our domestic ports of entry and in our Exclusive Economic Zone, to enforce our Nation's trade, safety, immigration, health, and security laws.
- Promoting Preparedness. Sustaining grant programs, to include the Port Security Grant Program, as part of DHS' comprehensive approach to strengthening the security and resilience of the United States through the systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber incidents, pandemics, and natural disasters.

### *Understanding the Risk*

In light of the central role that risk management plays in the DHS approach to promoting a secure, safe, efficient, and resilient supply chain, it is imperative that we continue to identify and understand risks within each component of the network and across the system as a whole. The evolving and dynamic nature of threats and vulnerabilities make this a challenging task.

DHS and the U.S. Government remain committed to preventing terrorist exploitation of the maritime supply chain or its components as a means of conducting a radiological or nuclear attack against the Nation. Since the authorization of the Domestic Nuclear Detection Office (DNDO) by the SAFE Port Act, DNDO has worked with partners from across the U.S. Government, including the Departments of Energy, State, Defense, Justice, the Intelligence

Community, and the Nuclear Regulatory Commission, to develop the Global Nuclear Domestic Architecture and implement its domestic component. The Global Nuclear Detection Architecture is a worldwide network of sensors, telecommunications, and personnel, with the supporting information exchanges, programs, and protocols that serve to detect, analyze, and report on nuclear and radiological material that are out of regulatory control. Specifically, DNDO coordinates with interagency partners and leads programs to develop technical nuclear detection capabilities, measure detector system performance, ensure effective response to detection alarms, and conduct transformational research and development for advanced detection technologies.

In particular, DNDO and other partners consistently review and update assessments of radiological/nuclear risks to maritime containerized cargo as well as other supply chain and non-supply chain pathways. The most recent analysis concluded that detection efforts focused on a single pathway, such as containerized maritime cargo, would not substantially reduce the overall risk of radiological/nuclear terrorism. Instead, DHS determined that a broader, multi-faceted and risk-based approach would better protect the United States. International scanning of maritime cargo is a key piece of this regime but is one of the many environments and pathways that DHS must consider and protect. As we continue to address radiological/nuclear threats in maritime cargo, we will view the risks through a broader lens and strive to reduce vulnerabilities across all pathways.

Based on this and similar risk assessments, the Secretary directed DHS to improve maritime container security in multiple areas in support of the intent of the SAFE Port Act. DHS, specifically CBP, will continue to refine targeting algorithms and rules within the Automated Targeting System to better identify high-risk containers warranting additional scrutiny. We will also work to increase the percentage of containers scanned abroad, with an emphasis on high-risk cargo, by prioritizing diplomatic engagement with host governments to increase their support of current Container Security Initiative operations and discuss potential expansion to additional key ports. And we will further explore potential new roles for industry stakeholders and/or international partners in scanning U.S.-bound maritime cargo containers.

#### *Advanced Information and Targeting*

Geospatially, our maritime security program begins overseas, in the hundreds of ports that ship goods directly to the United States and in the hundreds more that comprise the global supply chain network. Coast Guard personnel visit these foreign ports to assess their compliance with the International Ship and Port Facility Security (ISPS) Code. Vessels are also subject to the ISPS Code, and must maintain their security systems not only in port, but also while in transit. In addition to obtaining port or facility specific information, the Coast Guard requires vessel operators to provide advanced notice of arrival to the United States at least 96 hours before arrival in port. CBP has a similar requirement pertaining to cargo under the Importer Security Filing and Additional Carrier Requirements rule. Working together, the Coast Guard and CBP vet each vessel, which includes crew and cargo, arriving from overseas to produce a joint risk assessment and risk mitigation plan for each vessel. The Maritime Operational Threat Response (MOTR) Plan facilitates interagency coordination for situations requiring collaboration among multiple government agencies. Using this information, mitigation plans may include conducting

at-sea boardings, escorting vessels into port and other control measures for vessels, crews and cargoes to mitigate potential threats.

In addition, CBP and the Coast Guard process this advance information through the Automated Targeting System at the National Targeting Center for Cargo (NTC-C) before shipments reach the United States. This analytic process provides uniform review of cargo shipments for identification of the highest threat shipments, and presents data in a comprehensive, flexible format to address specific intelligence threats and trends. Through continuously updated targeting rules, and utilizing the latest intelligence information, the Automated Targeting System alerts the user to data that meets or exceeds certain predefined criteria.

The establishment of NTC-C in December 2001, and the development of partnerships and liaisons with other agencies, both domestically and abroad, has enabled real-time information sharing between agencies and governments. Partnerships with Immigrations and Customs Enforcement (ICE), the Drug Enforcement Administration (DEA), the Financial Crimes Enforcement Network (FinCEN), and the Departments of Commerce and Health and Human Services (HHS) promote information sharing and the exchange of best practices, while collaboration with foreign governments results in seizures and detection of threats at our borders and in foreign ports.

Utilizing advance information, targeting rules, and information sharing and partnerships, CBP has participated in a number of operations to interdict potentially illicit shipments.

- Through Project Synergy, NTC-C has identified more than 40 manufacturers in China involved in synthetic stimulant smuggling along with hundreds of U.S. and foreign consignees. This targeting and identification resulted in significant investigative value to active cases of DEA and ICE, as well as providing investigative leads resulting in the creation of new cases. This effort resulted in a total of 227 arrests, 416 search warrants executed and over \$51 million in assets seized.
- Working with ICE and our partners in Canada, Operation Envoy is an ongoing project which uses analytical data to develop narcotics targets and identify smuggling patterns through express consignment that transit the United States. This ongoing operation has netted six seizures and a total seizure weight of 17 kilograms of heroin.
- Project Zero Latitude was developed due to escalation of foreign and domestic narcotics interceptions involving sea containers of produce and seafood shipments particularly involving Ecuador. At the NTC-C, CBP conducted an analysis of historical ATS information and cocaine seizure data. The analysis enabled NTC-C to identify several smuggling trends that will facilitate the identification of future suspect shipments.

#### *Early Action Through Collaboration*

DHS and the State Department collaborate to establish effective partnerships with foreign countries. These partnerships greatly enhance DHS's collection of advance information and targeting efforts. No one in either the public or the private sector has the resources, the authority or the full range of expertise to ensure the security of the maritime transportation system in isolation. By understanding what needs to be done, we can together assess which stakeholder is

best positioned – and has the tools and resources – to do it. As the United States Government continues to implement the Strategy and advance other related efforts, industry and foreign government voices will remain critical to help inform the dialogue.

One example of a successful government-to-government partnership that has increased security in the years since the SAFE Port Act's release is the Container Security Initiative. Under this program, which was codified by the Act, CBP ensures that U.S.-bound maritime containers that pose a high risk are identified and inspected before they are placed on vessels destined for the United States. CSI operations in 58 foreign seaports provide a critical layer of security through collaboration for 80 percent of all incoming containerized cargo shipped to the United States.

As a result of the relationships established with host counterparts, CSI has augmented its original focus on terrorist-related risks by facilitating the interdiction of numerous illicit materials to include narcotics, pre-cursor chemicals, dual-use technology, stolen vehicles, weapons and ammunition, and counterfeit products. CSI capacity building efforts have allowed foreign Customs Administrations to develop risk-based targeting systems and provided training and guidance on anomaly identification using large scale NII technology. Working side-by-side with host counterparts allows the exchange of best practices, information, and collaboration on high-risk cargo, which further secures the global supply chain.

CBP's strong working relationships with our foreign partners is also demonstrated through the Secure Freight Initiative (SFI) in Qasim, Pakistan. Under this program, a team of remotely located CBP personnel assess U.S.-bound containers and request Pakistani Customs officials and Locally Engaged Staff to conduct physical exams when necessary. CBP officers use live video feeds streaming directly from Pakistan to the United States to monitor operations, including the physical examinations of containers. Port Qasim continues to showcase the SFI program in a country where the government and terminal operators support the initiative. From constructing the scanning site, to providing adequate staffing levels for SFI, the Government of Pakistan remains a strong partner in deploying SFI operations.

In addition to work with our foreign government partners, DHS also works with private industry to enhance security, while facilitating legitimate trade. One successful example is CBP's Customs Trade Partnership Against Terrorism (C-TPAT) program. Under C-TPAT, certain supply chain stakeholders, who volunteer to adopt strict security measures throughout their supply chains, receive benefits such as reduced or faster exams and designated personnel to assist with questions or problems. C-TPAT, established in 2001, has been a success – membership in this program has grown from seven companies in its first year to 10,718 as of May 1, 2014.

CBP is working with foreign partners to establish bi-national mutual recognition with C-TPAT. CBP currently has signed mutual recognition arrangements with Canada, the European Union, Japan, Jordan, Korea, New Zealand, and Taiwan (through an agreement between the American Institute in Taiwan and the Taipei Economic and Cultural Representative Office in the United States) and is continuing to work towards similar recognition with China, Israel, Mexico, Singapore, and other countries. These agreements create a unified and sustainable security

posture that can assist in securing and facilitating global cargo trade, while promoting end-to-end supply chain security.

DHS, through the U.S. Coast Guard, has also established successful partnerships with the range of state and local governments and organizations and with key private sector entities with maritime security responsibilities. One key example of these efforts are the Area Maritime Security Committees, chaired by the Captain of the Port, and responsible for the development of regional and port specific Area Maritime Security Plans to ensure adequate planning and preparation for a range of hazards and security concerns. As required by the SAFE Port Act, these plans include salvage and Maritime Transportation System recovery provisions to promote rapid recovery and stabilization after an incident. This focus on recovery demonstrates a maturing of our maritime security program and has paid dividends in several natural disaster events, including Hurricane Sandy in 2012. The port recovery operations that took place at the Port of New York and New Jersey were a model of public-private cooperation and enabled a much more rapid recovery than otherwise would have been possible. The Coast Guard has shared the lessons learned from that incident with other port areas across the country.

#### *Domestic Security Regimes*

In addition to deploying technology and personnel abroad under programs like CSI, DHS has made strides in strengthening detection equipment capabilities in domestic seaports. These systems help officers inspect containers and other cargo for radiological materials, illicit substances, and terrorist weapons. In fact 99 percent of all incoming containerized cargo arriving in the United States by sea is processed through a radiation portal monitor. In 2001, CBP had only 64 large-scale non-intrusive inspection systems and zero radiation port monitors. Today, CBP has 314 and 1,387 respectively. CBP has conducted over 68 million examinations using these technologies, resulting in over 15,800 narcotic seizures with a total weight of over 4.2 million pounds, and more than \$61.8 million in currency seizures.

The Coast Guard's layered defense against nuclear terrorism threats begins far from the nation's shores and includes inspection of foreign ports and vessels, employment of cutters, aircraft and boats offshore and in the nation's ports, and deployable specialized forces with global reach. The Coast Guard's unique authorities provide unparalleled access to maritime infrastructure and potential threats both offshore and in port. The Coast Guard conducts daily inspections and boardings to ensure vessels comply with maritime law and safety standards, applicable U.S. law and regulations, and control procedures for access to the nation's ports. All Coast Guard vessel boardings and inspection teams are equipped with nuclear/radiological detectors, with more than 72,000 boardings and 15,000 facility inspections conducted each year. The Coast Guard also has access to over 5,000 facilities for enforcement of safety and security requirements, with each boarding and inspection team playing a role in the nuclear detection architecture.

Also within U.S. ports, Coast Guard security regulations authorized by the SAFE Port Act and the Maritime Transportation Security Act (MTSA) require facilities, U.S. vessels, and designated foreign vessels calling on U.S. ports to conduct security assessments and to develop plans to address security vulnerabilities. The Transportation Worker Identification Credential (TWIC) is an important part of these efforts. The TWIC program 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. The TWIC program is the first and largest federal program to issue a standard biometric credential for use in diverse commercial settings across the nation. The nationwide applicability and recognition of TWIC promotes an economically efficient and mobile workforce, building efficiency in normal conditions and resilience when port disruptions occur. TWIC holders, with a legitimate business case to do so, may enter and work on vessels and facilities throughout the country.

TSA is responsible for enrollment, security threat assessments, and systems operations and maintenance related to TWIC cards. The Coast Guard is responsible for enforcement of TWIC card use at MTSA-regulated facilities and vessels. Efforts to secure our maritime environment can be complicated and, like our land and air borders, a layered approach is the best defense. TSA works closely with other DHS components to identify potential targets and design security measures to counter possible threats. Our work is collaborative and evolving. Since launching the program in October 2007, TSA has conducted comprehensive security threat assessments and issued cards to more than 2.9 million workers, including longshoremen, truckers, merchant mariners, and rail and vessel crews.

In addition, the Coast Guard conducts at least two security inspections annually at MTSA-regulated facilities, with one inspection being unannounced. This verifies that vessels and facilities in all Coast Guard Captain of the Port Zones are in compliance with TWIC requirements. 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. The 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.

Working closely with industry and our DHS partners, the TWIC program has evolved over the years to address concerns over the applicability of federal smart card best practices to a working maritime environment, such as the requirement for two trips to an enrollment center for card enrollment and activation. TSA restructured the program by launching OneVisit in June 2013, which provides workers the option to receive their TWIC through the mail rather than requiring a second visit for in-person card pickup and activation. Last month, TSA moved from the pilot phase of the program in Alaska and Michigan to a phased nationwide automated mailing system for all TWIC applicants who wish to receive their cards by mail.

TSA has also enhanced customer service by providing additional call center capacity for applicants checking on their enrollment status, enabling Web-based ordering for replacement cards, and strengthening quality assurance practices at enrollment centers. These critical customer service enhancements will support the next phase of the program as workers, initially enrolling five years ago, beginning to renew their TWIC cards for the next five-year span. Additionally, TSA is providing a streamlined multi-program enrollment experience at TSA enrollment centers across the country. This streamlined experience is a common sense efficiency that allows individuals to apply for our various credentialing programs, including TWIC, Hazardous Material Endorsement (HME) and TSA Pre✓™. Multi-program enrollment expands

the number of TWIC enrollment centers from the current 135 to over 300 this year, further providing a much needed convenience for workers.

*Promoting Preparedness*

MTSA regulated facilities, such as the Port of Long Beach, service approximately 95 percent of all trade to and from the United States, making them critically important to the flow of commerce and the nation's economy. Federal grant dollars are DHS's principal means of providing assistance to protect and enhance the security of the Nation's ports, waterways, and the commerce and traveling public that rely on those systems against acts of terrorism, major disasters, and other emergencies. Collectively, FEMA's preparedness grant programs have awarded more than \$38 billion in homeland security funds to states, urban areas, tribal and territorial governments, nonprofit agencies, and private sector organizations.

The Port Security Grant Program (PSGP), one of the grants most relevant to this hearing, has provided more than \$2.9 billion to port authorities, facility operators, and state and local agencies responsible for providing security services to U.S. ports. In fiscal year (FY) 2013, the PSGP provided more than \$93 million to 271 recipients within 81 distinct port areas across the United States and its territories. In FY 2014, \$100 million will be awarded through a competitive peer review process.

Although PSGP awards have always been risk-based and peer-reviewed, since FY 2013 a competitive element has also been added to PSGP funding decisions. The PSGP uses a two-tiered peer-review process designed to verify that projects address local port security needs as well as national priorities.

The U.S. Coast Guard Captain of the Port (COTP), in collaboration with the Area Maritime Security Committee, uses risk-based scoring criteria to conduct an initial review of proposed projects for the port area and make recommendations to FEMA. A national review panel consisting of officials from the Departments of Homeland Security and Transportation review applications and score the projects based on the COTP recommendation and how well the project addresses national priorities. Final funding recommendations are determined by factoring both the project effectiveness score and the port risk score, thus ensuring that the highest risk ports receive the bulk of the funding and that the funding goes toward projects that will most effectively mitigate risk within the port.

The over \$2.9 billion invested since the PSGP program's inception has made tangible progress in securing the Nation's port areas. For example, since 2006:

- More than \$161 million has been used to purchase equipment to enable port areas to achieve interoperable communications.
- More than \$344 million has been awarded to support over 600 portwide projects enhancing Maritime Domain Awareness (MDA) as well as enhancing portwide coordination and collaboration. This total includes enhanced portwide surveillance systems. For example, the Marine Exchange of Los Angeles used these funds to install cameras, as well as to fix lighting/solar-generated electrical systems and an

interoperability hub. This improved communications and made it easier to share information with other law enforcement and governmental agencies.

- Approximately \$267 million has been awarded for more than 500 vessel projects to increase port patrols and specialized vessels to enhance abilities to detect and respond to incidents involving chemical, biological, radioactive, and explosive devices. For example, the New York City Fire Department utilized more than 30 zodiac vessels that were purchased with PSGP funds to rescue approximately 1,000 people on the night that Hurricane Sandy made landfall.
- More than \$587 million has been awarded to support more than 1,385 facility security projects, to include installing fencing, lighting, cameras, gates, and TWIC readers. For example, many of these funds went toward securing liquid propane gas tanks in Delaware's ports.

As part of FEMA's effort and its strategic priority to posture and build capability for catastrophic disasters, the Administration has proposed the National Preparedness Grant Program (NPGP) and additional funding for NPGP in the Opportunity, Growth, and Security Initiative. The FY 2015 NPGP would work to more efficiently build and sustain core capabilities in the National Preparedness Goal, recognizing that a secure and resilient nation is one with the capabilities required, across the whole community, to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk. The NPGP draws upon and strengthens existing grants processes, procedures, and structures, emphasizing the need for greater collaboration and unity among Federal, state, local, tribal and territorial partners. Port security stakeholders will play a vital role in this collaborative effort. Area Maritime Security Committee members will participate in Urban Area Working Groups and State Senior Advisory Committees, thus providing them the opportunity to communicate port security risk information and NPGP funding needs relative to capability shortfalls specific to the needs of the port(s). The integrated governance processes of NPGP would help ensure that port stakeholders are not only well represented but are recognized as key contributors to the planning and analysis activities that go into making effective NPGP investments.

The NPGP would take a comprehensive, holistic, all-hazards approach in the spirit of the NPS, giving states the flexibility to determine where best to allocate grant funding based on their needs. NPGP could enhance existing collaboration between port stakeholders and non-port related entities and create greater understanding and appreciation of port area needs within the states. The integration of the PSGP into the NPGP is an important part of this proposal to allocate funds based on a strategic assessment of overall needs, requirements and capabilities, which is vital as the Agency works to make the most of its limited budget. This approach would allow resources to be targeted across the whole community rather than individual and separate sectors.

## **THE STRATEGIC CONTEXT**

### *The National Strategy for Global Supply Chain Security*

A significant milestone since the enactment of the SAFE Port Act was the release of the National Strategy for Global Supply Chain Security (Strategy) in early 2012. The Strategy established two

goals to strengthen the global supply chain system, including the maritime transportation network; namely, promoting the efficient and secure movement of legitimate goods, and fostering a global supply chain system that is resilient to natural as well as man-made disruptions. The Strategy also established the approach the United States Government will rely upon to achieve these goals – namely risk management and coordinated engagement with key stakeholders that have supply chain roles and responsibilities. These overarching goals of security/efficiency and resilience, and the stated focus on risk management and collaboration permeate all DHS port-related activities. They provide a common vision to enhance collaboration among components and with Federal partners and guide interactions with other key stakeholders.

### **CHALLENGES AHEAD**

The cornerstone of our mission at DHS is counterterrorism – that is, protecting the nation against terrorist attacks. We must remain vigilant in detecting and preventing terrorist threats that may seek to penetrate the homeland from the land, sea, or air. To address the terrorist threat and the other homeland security challenges the nation faces most collaboratively and effectively within the Department, we have recently undertaken an initiative entitled “Strengthening Departmental Unity of Effort.” In his April 22, 2014 memorandum, Secretary Johnson directed a series of actions to enhance the cohesiveness of the Department, while preserving the professionalism, skill, and dedication of the people within, and the rich history of, the DHS components.

The actions in this initiative: new senior leader forums led by the Secretary and the Deputy Secretary, and cross-departmental strategy, requirements, and budget development and acquisition processes that are tied to strategic guidance and informed by joint operational plans and joint operations are building and maturing DHS into an organization that is greater than the sum of its parts – one that operates much more collaboratively, leverages shared strengths, realizes shared efficiencies, and allows us to further improve our important role as an effective domestic and international partner.

Using the Unity of Effort lens, we will continue to focus on enhancing the capabilities of our components and our partners to address current and future challenges securing our ports. DHS’ approach to port security recognizes that our domestic ports function as critical hubs within complex global supply chain systems. DHS has devoted substantial attention and resources to implementing a layered, risk management approach to security across all transportation pathways. Ports are one key piece in a broad border construct, and security encompasses both overseas and inland facilities. Security does not end at the physical border.

Port security in an interconnected global system will continue to be a challenge. Two of the key issues we face are expanding trade and aging, inadequate infrastructure.

#### *Expanding Trade*

On September 9, 2013, World Trade Organization chief Roberto Azevedo announced that world trade was expected to grow by 2.5 percent that year, and by 4.5 percent in 2014. This was a reduction in the WTO’s previous 3.3 percent and 5 percent estimates, but it underscores that

even if the world trade doesn't grow as expected, it will grow. From a DHS perspective, growing trade volumes mean we must address additional demands for our services.

We expect that the Panama Canal expansion project, which opens in 2015, will impact mission activities by doubling the capacity of the canal, resulting in increased trade activity in United States ports. Numerous East Coast ports are investing in the necessary infrastructure. And as their cargo processing increases, our need to provide services without decreasing security will have to keep pace.

Similarly, as Arctic conditions change and more open water is available for transport for longer periods of the year, trade will shift to shorter northern routes. Previously unavailable natural resources will be exploited. DHS will be challenged to provide services in extreme conditions, including: search and rescue; port and facility security; and environmental protection. On the North Slope, there are more than 200,000 square miles of Arctic water over which we have jurisdiction that will see a steady increase in activity. Solutions to this increased demand in times of declining budgets must rely on efficient use of the resources at our disposal, closer partnerships with the private sector, and refinement of our strategy of risk segmentation to focus on the greatest risks.

#### *Aging Infrastructure*

In the face of increasing trade and shifting trade patterns, we must confront aging infrastructure. The Coast Guard has been recapitalizing its assets for a number of years, procuring new cutters, aircraft, and communications systems with Congressional support. We thank you for your continued support. CBP and the Domestic Nuclear Detection Office also face challenges with aging assets. Our Non-Intrusive Inspections (NII) and Radiation Portal Monitor (RPM) systems have operational life-spans of approximately 10-13 years. Many are now approaching their end of service life, and we are attempting to increase NII effectiveness by deploying them more strategically, in response to trade flow patterns. Those systems will have to be recapitalized. We hope that Congress will support us in that effort.

DHS and its components have implemented with great success many initiatives to promote the security, efficiency, and resilience of the nation's ports and meet the challenges posed by increasing volumes of trade, limited resources and aging assets.

#### *International Trade Data System and Trade Facilitation*

An integral part of our strategy to address these challenges with increased efficiency is the completion of the International Trade Data System. As the United States' single window system for import and export data, this system will enable traders to provide data on time, through one portal, electronically. The capability will also improve efficiencies for government stakeholders. Shifting to electronic submission allows the 47 departments and agencies with cargo import and export requirements to automatically process documentation, make cargo release and clearance decisions, and conduct risk assessments to guide appropriate enforcement activities. By being more efficient, we will improve enforcement of, and compliance with, our Nation's trade, security, safety, and environmental laws.

*Perimeter Security*

Recognizing that maritime cargo destined for the United States often travels through Canada, and vice versa, DHS will continue to embrace the concept of perimeter security that is the core of President Obama and Prime Minister Harper's *Beyond the Border* declaration. Cooperation with our northern partners to harmonize our security regimes will allow either party to target arriving cargo, with inspections completed at the original port of entry. Inspecting once, and clearing twice, will be a marked improvement in efficiency on both sides of the border.

In the past year, we made good progress toward the perimeter approach, through the release of an Integrated Cargo Security Strategy that supports efforts to address, as early as possible, risks associated with maritime shipments arriving from offshore. We conducted pilot projects at Prince Rupert, British Columbia, Montreal, Quebec, and Newark, New Jersey. We also released the first joint Border Infrastructure Investment Plan, reflecting a mutual understanding of recent, ongoing, and planned border infrastructure improvements and confirmation of Canada's immediate investment plans at key border crossings.

We have also collaborated extensively with our southern partner, Mexico, through such efforts as the 21<sup>st</sup> Century Border Initiative and bilateral support. In keeping with our end-to-end supply chain security efforts, CBP was extensively involved in the design and deployment of Mexico's New Scheme of Certified Companies (Nuevo Esquema de Empresas Certificada, or NEEC). Introduced in January, 2012, the program is a virtual twin to our C-TPAT program. And we have, with Congress' support, invested in border infrastructure to increase efficiency and security at such ports of entry as San Ysidro and Laredo.

*Cyber Security*

Cyber security is another growing security concern, and the Coast Guard is using existing authorities to identify and address how cyber events can threaten the Marine Transportation System (MTS). The Coast Guard has directed our Area Maritime Security Committees to evaluate how cyber events might impact their port areas, and provided extensive information to industry on the National Institute of Standards and Technology Framework and other cyber security best practices. We have directed MTSA regulated vessel and facility operators to report cyber related breaches of security and suspicious activity to the Coast Guard. Working closely with Industrial Control Systems Cyber Emergency Response Team and other DHS Offices, the Coast Guard has provided extensive information to the maritime industry about cyber threats, self-evaluation tools, training opportunities, and other resources. The Coast Guard is also working with the Department of Energy to adopt some of their best practices and evaluation tools for the maritime industry. MTSA regulated vessels and facilities are required to include computer systems and networks in their security assessments and security plans. The Coast Guard is developing standard response and communication procedures for our Captains of the Port to follow in the event of a cyber-attack or event. The Coast Guard will continue to integrate cyber risks into our existing security regime in order to reduce vulnerabilities and promote effective response and recovery operations.

**CONCLUSION**

Port security is a challenging, dynamic mission. To manage it effectively and avoid an “end zone defense” strategy, requires layered efforts coordinated across the DHS enterprise that reach back as far into the global supply chain system as possible. Our objective is to protect our ports through making sure that U.S.-bound vessels are secure before they depart and during their voyage, that they are carrying safe, secure cargo and people, into secure ports. Working with our Federal partners and our domestic and international stakeholders in the public and private sector, CBP’s cargo security programs help to safeguard the Nation’s economic strength and competitiveness.

With the implementation of MTSA and SAFE Port Act, DHS and its various components have made great strides to manage the risks posed to the MTS and other critical infrastructure by external elements. Managing this risk has entailed the creation of a framework that uses a layered strategy to vet transportation workers, vessels, cargo and crew, beginning at international origin and continuing throughout the global supply chain. These efforts also require companies, vessels, facilities and other port stakeholders to examine and address potential vulnerabilities.

Thank you for the opportunity to appear before you today to discuss these important issues, Mr. Chairman. We look forward to answering any questions you or other members of the Committee may have.



United States Government Accountability Office

---



Testimony  
Before the Committee on Homeland  
Security and Governmental Affairs,  
U.S. Senate

---

For Release on Delivery  
10:30 a.m. ET  
Wednesday, June 4,  
2014

## MARITIME SECURITY

### Progress and Challenges with Selected Port Security Programs

Statement of Stephen L. Caldwell, Director, Homeland  
Security and Justice

## GAO Highlights

Highlights of GAO-14-636T, a testimony before the Senate Committee on Homeland Security and Governmental Affairs

### Why GAO Did This Study

Ports, waterways, and vessels handle billions of dollars in cargo annually, and an attack on our nation's maritime transportation system could have dire consequences. Ports are inherently vulnerable to terrorist attacks because of their size, general proximity to metropolitan areas, the volume of cargo being processed, and their link to the global supply chain—that is, the flow of goods from manufacturers to retailers. Balancing security concerns with facilitation of the free flow of people and commerce remains an ongoing challenge for federal, state, local, and private stakeholders operating in ports.

Within DHS, several components are responsible for port security activities. These activities include, among other things, promoting maritime domain awareness, conducting port facility inspections, and screening incoming vessels' cargoes for the presence of contraband such as weapons of mass destruction, illicit drugs, or explosives.

This statement discusses progress and challenges in key areas of DHS port security programs. It is based on work GAO has previously conducted from September 2003 to September 2013 with selected updates conducted through May 2014. For these updates, GAO contacted DHS officials and reviewed relevant documents.

### What GAO Recommends

In prior reports, GAO has made recommendations to DHS to strengthen various port security programs. DHS generally concurred with the recommendations and has taken actions, or has actions under way, to address most of these recommendations.

View GAO-14-636T. For more information, contact Stephen L. Caldwell at (202) 512-9610 or [CaldwellS@gao.gov](mailto:CaldwellS@gao.gov)

June 4, 2014

## MARITIME SECURITY

### Progress and Challenges with Selected Port Security Programs

#### What GAO Found

GAO's prior work has shown that the Department of Homeland Security (DHS) and its component agencies—particularly the Coast Guard and Customs and Border Protection (CBP)—have made substantial progress in three key areas of port security since the September 11, 2001 terrorist attacks (9/11), but some challenges remain.

**Maritime domain awareness and information sharing.** DHS agencies along with other port partners have taken actions to enhance visibility over the maritime domain and facilitate cooperation among partners by collecting, assessing and sharing key information. However, some challenges remain in implementing the tools necessary to maintain this focus and increase coordination among stakeholders. For example, in multiple reports since 2011, GAO found the Coast Guard's weak management of technology acquisitions—that were focused on enhancing maritime awareness and increasing communication among partners—resulted in these acquisitions not fully achieving their intended purposes. DHS concurred with GAO's recommendations for addressing these weaknesses.

**Security in domestic ports.** Since 9/11, DHS components have taken a wide variety of actions to better secure domestic ports. For example, the Coast Guard has assessed risks to cruise ships in accordance with DHS guidance and is providing escorts for high-risk vessels such as cruise ships and ferries while CBP is reviewing passenger and crew data to target inspections. In addition, since 2002, the Federal Emergency Management Agency (FEMA) has provided almost \$2.9 billion in federal funding through the Port Security Grant Program (PSGP) to help defray the cost of implementing security efforts in many ports and has established measures to improve the administration of the PSGP. However, in 2014 FEMA stated that it is unable—due to resource constraints—to annually measure reduced vulnerability attributed to enhanced PSGP-funded security measures. Meanwhile, the Transportation Security Administration (TSA) and the Coast Guard have been administering a program requiring maritime workers to obtain a biometric identification card to gain access to certain facilities. However, in 2011, GAO recommended that DHS assess internal controls to identify actions needed to address, among other things, weaknesses governing enrollment and background checks. As of March 2014 this action had not been completed.

**Protection of the global supply chain.** DHS agencies, especially CBP, have taken steps to enhance the security of the global supply chain—particularly for cargo bound for the United States. Efforts have focused on assessing and mitigating cargo risk before it enters U.S. ports by better targeting and scanning cargo, and establishing security partnerships with the foreign countries and companies that ship cargo to the United States. However, in multiple reports since 2005, GAO found that DHS programs focused on protecting the global supply chain have been implemented with varying degrees of success and that many would benefit from the DHS agencies conducting further assessments of the programs, among other things. GAO has made recommendations to address these issues and DHS has concurred or generally concurred with most of these recommendations and has taken actions to address many of them.

---

Chairman Carper, Ranking Member Coburn, and Members of the Committee:

Thank you for the opportunity to discuss the Department of Homeland Security's (DHS) ongoing port security efforts and programs. Ports, waterways, and vessels handle billions of dollars in cargo annually, and an attack on our nation's maritime transportation system could have dire consequences. Ports are inherently vulnerable to terrorist attacks because of their size, general proximity to metropolitan areas, the volume of cargo being processed, and the ready access the ports have to transportation links into the United States. An attack on a large port could also have a widespread impact on the broader global supply chain—the flow of goods from manufacturers to retailers—and the world economy. Balancing security concerns with the need to facilitate the free flow of people and commerce remains an ongoing challenge for federal, state, local, and private stakeholders operating in ports.

Within DHS, several components, including the Office of Policy, the U.S. Coast Guard, U.S. Customs and Border Protection (CBP), the Transportation Security Administration (TSA), the Domestic Nuclear Detection Office (DNDO), and the Federal Emergency Management Agency (FEMA) are responsible for port security activities. These activities include, among other things, promoting maritime domain awareness, conducting port facility and commercial vessel inspections, and screening incoming vessels' cargoes for the presence of contraband such as weapons of mass destruction (WMD), illicit drugs, or explosives, while facilitating the flow of legitimate trade and passengers.

My statement today discusses progress and challenges with DHS programs responsible for enhancing port security. Specifically, I will address maritime domain awareness and information sharing, security in domestic ports, and protection of the global supply chain.

My statement is based on reports and testimonies we issued from September 2003 through September 2013 related to maritime, port, vessel, and cargo security—with selected updates on how DHS responded to our prior recommendations, which we conducted through May 2014. To perform the work for our previous reports and testimonies, we visited domestic and overseas ports; reviewed agency program documents, port security plans, and other documents; and interviewed officials from the federal, state, local, private, and international sectors, among other things. The officials we met with represented a wide variety of stakeholders including the Coast Guard, CBP, port authorities, terminal

---

operators, vessel operators, foreign governments, and international trade organizations. For the selected updates, we contacted DHS officials and reviewed relevant documents pertaining to the status of recommendation implementation. Further details on the scope and methodology for the previously issued reports and testimonies are available within each of the published products. A list of products on which this statement is based is included at the end of the statement. We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

## Background

---

### Legislation, Strategies, and Plans

Since the terrorist attacks of September 11, 2001 (9/11), Congress established a new port security framework—much of which was set in place by the Maritime Transportation Security Act of 2002 (MTSA) and the Security and Accountability For Every Port Act of 2006 (SAFE Port Act).<sup>1</sup> This framework is implemented through various strategies and plans, and the combined efforts of several DHS components.

Enacted in November 2002, MTSA was designed, in part, to help protect the nation's ports and waterways from terrorist attacks by requiring a wide range of security improvements. Among the major requirements included in MTSA were (1) conducting vulnerability assessments for port facilities and vessels; (2) developing security plans to mitigate identified risks for ports, port facilities, and vessels; (3) developing a biometric identification card to help restrict access to secure areas to only authorized personnel; and (4) establishing a process to assess the security levels of foreign ports from which vessels depart on voyages to the United States.

In 2006, the SAFE Port Act, which in part amended MTSA, became law. The SAFE Port Act required DHS to develop, implement, and update, as appropriate, a strategic plan to enhance the security of the international supply chain—the flow of goods from manufacturers to retailers. Further,

---

<sup>1</sup>Pub. L. No. 107-295, 116 Stat. 2064; Pub. L. No. 109-347, 120 Stat. 1884.

---

the SAFE Port Act required DHS to establish pilot projects at three ports to test the feasibility of scanning 100 percent of U.S.-bound cargo containers at foreign ports.

The federal government has made progress in national and port-level security planning by developing strategies and plans. Specifically, the National Strategy for Maritime Security, published in September 2005, aimed to align all federal government maritime security programs and activities into a comprehensive and cohesive national effort involving appropriate federal, state, local, and private sector entities.<sup>2</sup> Further, the Coast Guard has developed Area Maritime Security Plans (AMSP) to enhance the security of domestic ports around the country. Applicable governmental and private entities contribute to the AMSPs, which serve as the primary means to identify and coordinate Coast Guard procedures related to prevention, protection, and security response.

---

#### Roles and Responsibilities

DHS is the lead federal department and with its component agencies has responsibility for administering much of the port security framework. DHS and its components must balance security priorities with the need to facilitate legitimate trade through the efforts of several component agencies. DHS components with port security responsibilities include:

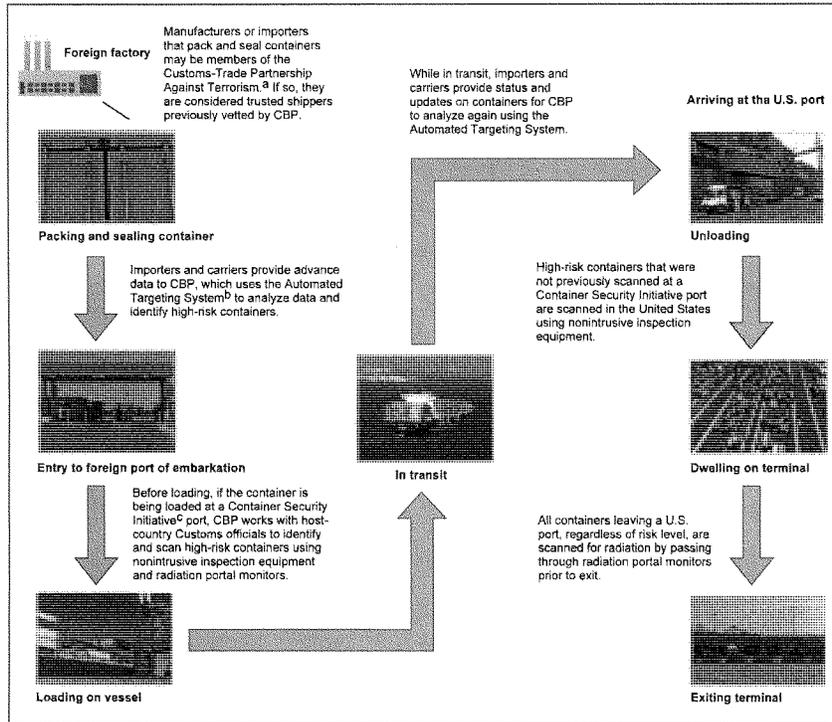
- **Office of Policy:** The Office of Policy leads the coordination, integration, and development of DHS-wide policies, programs, strategies, and plans.
- **U.S. Coast Guard:** The Coast Guard, among other things, conducts port facility and commercial vessel inspections and leads the coordination of maritime information-sharing efforts.
- **TSA:** TSA has lead responsibility for managing the Transportation Worker Identification Credential program, which is designed to control the access of maritime workers to regulated maritime facilities in the United States.

---

<sup>2</sup>Homeland Security Presidential Directive 13 (HSPD-13) directed the Secretaries of Defense and Homeland Security to lead a joint effort to draft the national strategy. HSPD-13 also directed DHS to develop eight supporting implementation plans to address the specific threats and challenges of the maritime environment. These plans include overarching strategies such as the *National Plan to Achieve Maritime Domain Awareness* and are implemented by specific plans such as the *Countering Piracy off the Horn of Africa: Partnership & Action Plan*.

- 
- **DNDO:** DNDO is responsible for acquiring and supporting the deployment of radiation detection equipment, including radiation portal monitors at domestic seaports, to support the scanning of cargo containers before they enter U.S. commerce.
  - **FEMA:** FEMA is responsible for administering grants to improve the security of the nation's highest-risk port areas.
  - **CBP:** CBP is responsible for the screening of incoming vessels' crew and cargoes for the presence of contraband, such as WMDs, illicit drugs, or explosives. As shown in figure 1, CBP programs are involved throughout the global supply chain process.

Figure 1: Global-Supply Chain Process



Source: GAO (analysis); GAO and DHS S&T (photos); Art Explosion (clipart). | GAO-14-636T

<sup>8</sup>The Customs-Trade Partnership Against Terrorism is a voluntary program designed to improve the security of the international supply chain while maintaining an efficient flow of goods. Under this program, CBP officials work in partnership with private companies to review their supply chain security plans to improve members' overall security.

<sup>2</sup>The Automated Targeting System is a mathematical model that uses weighted rules to assign a risk score to arriving cargo shipments based on shipping information. CBP uses the Automated Targeting System as a decision support tool in targeting cargo containers for inspection.

<sup>3</sup>The Container Security Initiative places CBP staff at participating foreign ports to work with host country customs officials to target and examine high-risk container cargo for WMDs before it is shipped to the United States. CBP officials identify the containers that may pose a risk for terrorism and request that the officials' foreign counterparts examine the contents of the containers.

### DHS Has Made Substantial Progress in Enhancing Port Security, but Challenges Remain

Our prior work has shown that DHS and its component agencies—particularly the Coast Guard and CBP—have made substantial progress in implementing various programs that, collectively, have enhanced port security but some challenges remain. Examples of progress and challenges in the areas of (1) enhancing maritime domain awareness and information sharing, (2) increasing security in domestic ports, and (3) protecting the global supply chain are discussed below.

#### Maritime Domain Awareness and Information Sharing

DHS, its component agencies, and other port partners have taken a variety of actions to enhance visibility of the maritime domain and facilitate cooperation among partners by collecting, assessing and sharing key maritime domain information, but challenges remain. Timely awareness of the maritime domain, and knowledge of threats helps the Coast Guard and other agencies to detect, deter, interdict, and defeat adversaries.

- **Interagency operations centers:** Interagency operations centers (IOCs) are physical or virtual centers of collaboration to improve maritime domain awareness and operational coordination among port partners—including federal, state, and local law enforcement agencies. Port partners are able to use these centers to participate in maritime security activities, such as the implementation and administration of intelligence activities, information sharing, and vessel tracking. The SAFE Port Act required the establishment of certain IOCs, and the Coast Guard Authorization Act of 2010 further specified that IOCs must provide, where practicable, for the physical colocation of the Coast Guard with its port partners, and that IOCs must include information management systems.<sup>3</sup> In February 2012, we reported that the Coast Guard is continuing its efforts to establish IOCs at 35 locations and share maritime domain awareness information with its port partners.<sup>4</sup> However, we identified

<sup>3</sup>46 U.S.C. § 70107a.

<sup>4</sup>GAO, *Maritime Security: Coast Guard Needs to Improve Use and Management of Interagency Operations Centers*, GAO-12-202 (Washington, D.C.: Feb. 13, 2012).

---

factors that jeopardized the centers from meeting their purpose of improving information sharing and enhancing maritime domain awareness across federal, state, and local port partners, including weak management of the Interagency Operations Center Acquisition Project which was to provide information-management tools to improve interagency coordination, enhance awareness, and automate anomaly detection. As a result, we made five recommendations to address these issues—including recommendations related to improving the Coast Guard's process for collecting data and incorporating port partners' input into the development of requirements for an information-management and sharing system that would facilitate the IOCs. The Coast Guard concurred with these recommendations but has not implemented them, stating that neither the President's fiscal year 2013 nor fiscal year 2014 budget requested resources for the Interagency Operations Center Acquisition Project.

- **Common Operating Picture:** In general, the Coast Guard's Common Operating Picture (COP) can be described as a map-based information system—that can be shared among Coast Guard commands—that displays vessels, information about those vessels and the environment surrounding them. As a way to display COP information, the Coast Guard in 2010 deployed the Enterprise Geographic Information System (EGIS).<sup>5</sup> However as we reported in April 2013, there have been numerous issues with EGIS.<sup>6</sup> For example, Coast Guard information technology (IT) officials told us they had experienced challenges in meeting its goals for the system largely related to insufficient computational power on some Coast Guard workstations, a lack of training for users and system installers, and inadequate testing of EGIS software before installation. Consequently, the Coast Guard began developing a new COP-related technology, Coast Guard One View (CG1V). However, as we also reported in our April 2013 report, the Coast Guard did not follow its own IT development guidance when implementing CG1V. As a result, we recommended that the Coast Guard issue guidance clarifying the application of the System Development Life Cycle (SDLC) for the development of future projects. The Coast Guard concurred with the

---

<sup>5</sup> EGIS is the Coast Guard's geographic information system used to view and manage information about geographic places, analyze spatial relationships, and model spatial processes.

<sup>6</sup> GAO, *Coast Guard: Clarifying the Application of Guidance for Common Operational Picture Development Would Strengthen Program*, GAO-13-321 (Washington, D.C.: Apr. 25, 2013).

---

recommendation and reported that it planned to issue guidance and clarify procedures regarding the applicability of the SDLC. In January 2014, the Coast Guard updated its SDLC tailoring plan. We reviewed the updated plan and determined that while it represented progress, it did not fully meet the intent of our recommendation because it was focused narrowly on the COP acquisition rather than more broadly clarifying procedures regarding the applicability of the SDLC for other IT projects as well. As a result, this recommendation remains open.

- **Vessel and aircraft maritime domain awareness:** To further enhance its ability to monitor the maritime domain, the Coast Guard planned to build a command, control, communication, computers, intelligence, surveillance, and reconnaissance (C4ISR) system and put this system on all of its planes and larger vessels.<sup>7</sup> This system was designed to improve the probability of executing a successful mission by increasing the speed and accuracy of the Coast Guard's process of surveying the maritime domain, detecting and classifying targets, and then responding to the situation. A planned system-of-systems concept was intended to connect Coast Guard assets through a single command and control architecture—C4ISR.<sup>8</sup> However, in July 2011, we reported that the Coast Guard had not met its goal of building the \$2.5 billion C4ISR system.<sup>9</sup> Specifically, we reported that the Coast Guard had repeatedly changed its strategy for achieving the C4ISR system's goal of building a single fully interoperable command, control, intelligence, surveillance, and reconnaissance system across the Coast Guard's new vessels and aircraft. Further, we found that not all aircraft and vessels were operating the same C4ISR system, or even at the same classification level, and hence could not directly exchange data with one another. Given these uncertainties, we concluded that the Coast Guard did not have a clear vision of the C4ISR required to meet its missions. In response to our recommendation, the Coast Guard has developed needed documentation and truncated portions of the program. The Coast Guard is now working toward the goal of developing compatible and

---

<sup>7</sup>In July 2011, we reported that the Coast Guard was developing C4ISR infrastructure that it expected to collect, correlate, and present information into a single COP to facilitate mission execution. See GAO, *Coast Guard: Action Needed as Approved Deepwater Program Remains Unachievable*, GAO-11-743 (Washington, D.C.: July 28, 2011).

<sup>8</sup>A system-of-systems is a set or arrangement of assets that results when independent assets are integrated into a larger system that delivers unique capabilities.

<sup>9</sup>GAO-11-743.

---

manageable software packages on major cutters and medium-and long-range planes. We will continue to assess the C4ISR program through our ongoing work on Coast Guard recapitalization efforts and expect to issue a report in summer 2014.

---

**Security in Domestic Ports** Port stakeholders and DHS component agencies have implemented a wide variety of security measures that are intended to better secure U.S. ports. For example, in 2003, the Coast Guard issued regulations requiring offshore facility and port and operators to enhance their own security through the implementation of security plans for their facilities.<sup>10</sup> Further, the Port Security Grant Program was established in 2002, and through FEMA's management of this program, federal grant funding is made available to states, localities and private parties to help defray the costs of required security measures. Other security measures directly involving DHS agencies include Coast Guard inspections and escorts of high-risk vessels, among other actions.

- **Port and offshore facility security plans and inspections:** To enhance the security of port facilities, the Coast Guard has implemented regulations and programs requiring port facility security plans. Owners and operators of certain maritime facilities are required to conduct assessments of security vulnerabilities, develop security plans to mitigate these vulnerabilities. The Coast Guard inspects these facilities annually. In addition to inspecting port facilities, the Coast Guard also conducts inspections of offshore facilities, such as oil rigs. In our October 2011 report on inspections of offshore energy facilities, we found that the Coast Guard had taken actions to help ensure the security of offshore energy facilities, such as developing and reviewing security plans, but faced difficulties ensuring that all facilities complied with requirements.<sup>11</sup> We recommended that the Coast Guard develop policies and procedures to ensure that annual security inspections are conducted and information entered into databases is more useful for management. The Coast Guard concurred with these recommendations and is in the process of updating its guidance for Coast Guard units and program managers. In February 2014, Coast Guard officials told us that the Coast Guard plans to improve its inspection database by March 2015.

---

<sup>10</sup> 33 C.F.R. §§ 105.400-415, 106.400-415.

<sup>11</sup> GAO, *Maritime Security: Coast Guard Should Conduct Required Inspections of Offshore Energy Infrastructure*, GAO-12-37 (Washington, D.C.: Oct. 26, 2011).

- 
- **Port Security Grant Program:** To help defray some of the costs of implementing security at ports around the United States, the Port Security Grant Program was established in January 2002 and since then has awarded almost \$2.9 billion for port security efforts.<sup>12</sup> The Port Security Grant Program awards funds to states, localities, and private port stakeholders to strengthen the nation's ports against risks associated with potential terrorist attacks. We reported in November 2011 that, for fiscal years 2010 and 2011, allocations of these funds were based on DHS's risk model and implementation decisions were made largely in accordance with risk.<sup>13</sup> For example, we found that allocations of funds to port areas were highly positively correlated to port risk, as calculated by DHS's risk model. However, we also noted that the method used to calculate vulnerability—a port's relative exposure to an attack—could be strengthened to better account for how the implementation of grant-funded security projects affects a port's vulnerability score. Accordingly, we recommended that DHS develop a vulnerability index that accounts for how security improvements affect port vulnerability, and incorporate these changes into future iterations of the grant's risk model. In February 2014, FEMA officials stated that they have determined that this specific enhancement is not achievable, in part because the agency lacks the resources to annually measure the reduced vulnerability attributed to enhanced PSGP security measures. However, they also stated that FEMA remains committed to improving the measure of vulnerability within the grant's risk model. In our 2011 report, we also raised questions about the effectiveness of the administrative management of the grant program, and we recommended that FEMA develop timeframes and related milestones for implementing performance measures. In February 2014, FEMA officials provided documentation of management and administrative performance measures to help strengthen the implementation, administration and oversight of the PSGP, and thus we have closed this recommendation.
  - **Personnel access to port facilities:** The Transportation Worker Identification Credential (TWIC) program, administered by TSA and the Coast Guard, requires maritime workers to undergo background checks and obtain a biometric identification card to gain unescorted access to

---

<sup>12</sup>Pub. L. No. 107-117, 115 Stat. 2230, 2327 (2002). MTSA codified the program when it was enacted in November 2002. 46 U.S.C. § 70107.

<sup>13</sup>GAO, *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened*, GAO-12-47 (Washington, D.C.: Nov. 17, 2011).

---

secure areas of regulated maritime facilities. Initiated in December 2001, we have been reporting on TWIC progress and challenges since September 2003.<sup>14</sup> Among other issues, we have highlighted steps that TSA and the Coast Guard have taken 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 the Coast Guard from August 2004 through June 2005. We also identified challenges related to ensuring that the TWIC technology works effectively in the harsh maritime environment.<sup>15</sup>

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.<sup>16</sup> As a result, we recommended that the DHS components implementing the pilot—TSA and Coast Guard—develop an evaluation plan to guide the remainder of the pilot and identify how they will compensate for areas where the TWIC reader pilot would not provide the information. DHS agreed and took initial steps, but did not develop an evaluation plan, as we recommended. 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 MTA-regulated facilities is restricted to qualified individuals.<sup>17</sup> Accordingly, in our 2011 report, we recommended that DHS assess TWIC program internal controls to identify needed corrective actions, assess TWIC's effectiveness, and use the information to identify effective and cost-efficient methods for meeting program objectives. While DHS concurred with our recommendation, as

---

<sup>14</sup>GAO, *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain*, GAO-03-1155T (Washington, D.C.: Sept. 9, 2003).

<sup>15</sup>GAO, *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, GAO-06-982 (Washington, D.C.: Sept. 29, 2006). TWIC readers and related technologies operated outdoors in the harsh maritime environment can be affected by dirt, salt, wind, and rain.

<sup>16</sup>GAO, *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers*, GAO-10-43 (Washington, D.C.: Nov. 18, 2009).

<sup>17</sup>GAO, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, GAO-11-657 (Washington, D.C.: May 10, 2011).

---

of May 2013 DHS had not taken significant action to address our recommendation. We therefore reaffirmed this recommendation in May 2013, recommending to Congress that it repeal a requirement that DHS issue regulations consistent with the TWIC reader pilot and instead require DHS to complete an assessment that evaluates the effectiveness of using TWIC with readers for enhancing port security, and then use the results of the assessment to promulgate a final regulation as appropriate.<sup>18</sup>

In January 2014, the explanatory statement accompanying the Consolidated Appropriations Act, 2014, directed DHS to complete the TWIC program assessment that we recommended within 90 days after the enactment of the Consolidated Appropriations Act of 2014 (by April 17, 2014).<sup>19</sup> As of March 2014, DHS had taken steps toward addressing our 2011 recommendation, such as developing a list of control issues we identified in 2011 and establishing an Executive Steering Committee to address the recommendations. However, TSA had no estimate for when the effectiveness assessment would be completed.

- **Operations and escorts:** To further protect ports, DHS agencies assess risks, conduct inspections, and escort high-risk vessels. For example, the Coast Guard has assessed risks to cruise ships in accordance with DHS guidance—which requires that the agency analyze threats, vulnerabilities, and consequences. CBP reviews passenger and crew data to help target inspections. In addition, the Coast Guard escorts a certain percentage of high-capacity passenger vessels—cruise ships, ferries, and excursion vessels—to protect against external threats, such as a waterborne improvised explosive device. Specifically, the Coast Guard has provided escorts for cruise ships to help prevent waterside attacks and has provided a security presence on passenger ferries during their transits. Further, the Coast Guard has conducted energy commodity tanker security activities, such as security boardings, escorts, and

---

<sup>18</sup>GAO, *Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed*, GAO-13-198 (Washington, D.C.: May 8, 2013).

<sup>19</sup>Explanatory statement accompanying Consolidated Appropriations Act, 2014, Pub. L. No. 113-76, 128 Stat. 5.

---

patrols. Such actions enhance the security of these vessels, thereby also protecting the ports in which they operate.<sup>20</sup>

---

**Protection of the Global Supply Chain**

DHS agencies have also taken steps to enhance the security of cargo bound for the United States—even before it arrives in U.S. ports. Some of these efforts have focused on increasing the volume, accuracy and timing of information available to DHS agencies for assessing cargo risk. Other efforts have involved an increased use of technology such as scanners. DHS agencies have also taken steps to enhance U.S. port security by establishing security measures and partnerships with the foreign countries and companies that ship cargo to the United States—so that cargo risk is assessed and mitigated before the cargo may enter U.S. ports. These various measures and programs have been implemented with varying degrees of success.

- **Cargo screening and the Automated Targeting System:** As part of its efforts to target high-risk maritime cargo containers for inspection, CBP screens containers in advance of their arrival in the United States. To enhance the screening of these containers, DHS developed the Automated Targeting System (ATS)—a computerized system that assesses information on each U.S.-bound cargo shipment and assigns it a risk score. CBP officers then use this risk score, along with other information, such as the shipment's contents, to determine which shipments to physically examine. In September 2010, we reported that CBP had made progress in implementing ATS and enhancing it through the use of additional data.<sup>21</sup> However, in 2012, we also found that more regular assessments of ATS were needed to enhance its targeting of maritime cargo containers and better position CBP to provide reasonable assurance of the effectiveness of ATS. We therefore recommended that the Commissioner of CBP (1) ensure that future updates to the rules that

---

<sup>20</sup>For additional information on the Coast Guard's role in protecting and/or escorting certain vessels, please see the following GAO reports: GAO, *Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain*, GAO-10-400 (Washington, D.C.: Apr. 9, 2010); *Maritime Security: Ferry Security Measures Have Been Implemented, but Evaluating Existing Studies Could Further Enhance Security*, GAO-11-207 (Washington, D.C.: Dec. 3, 2010); *Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers*, GAO-08-141 (Washington, D.C.: Dec. 10, 2007).

<sup>21</sup>GAO, *Supply Chain Security: CBP Has Made Progress in Assisting the Trade Industry in Implementing the New Importer Security Filing Requirements, but Some Challenges Remain*, GAO-10-841 (Washington, D.C.: Sept. 10, 2010).

---

identify risks are based on results of assessments that demonstrate the effectiveness of such updates; and (2) establish targets for CBP's performance measures and use those measures to assess the effectiveness of ATS on a regular basis to better determine when updates to the rules that identify risks are needed.<sup>22</sup> CBP concurred with the recommendations and in May 2014 provided milestones for implementing the recommendations by June 2015.

- **Deploying scanning technologies:** Once cargoes such as those shipped in containers arrive in U.S. ports, DHS deploys various technologies to scan their contents. DHS technological improvements have been focused on developing and deploying equipment to scan cargo containers for nuclear materials and other contraband to better secure the supply chain. Specifically, to detect nuclear materials, CBP, in coordination with DNDO, has deployed over 1,400 radiation portal monitors at U.S. ports of entry. Most of the radiation portal monitors are installed in primary inspection lanes through which nearly all traffic and shipping containers must pass. These monitors trigger an alarm when they detect radiation coming from a vehicle or shipping container. CBP then conducts further inspections at its secondary inspection locations to identify the cause of the alarm and determine whether there is a reason for concern. In 2005, DNDO began working with CBP on a program to develop and test a type of next-generation radiation portal monitor—the advanced spectroscopic portal (ASP)—designed to both detect radiation and identify the source as benign, suspect, or a threat.<sup>23</sup> The initial concept of the program was to develop, procure, and deploy enough ASPs to replace many of CBP's currently deployed radiation portal monitors and handheld detectors at a cost of \$2 billion to \$3 billion, according to DNDO. However, in 2007, we found that the initial testing related to DNDO's efforts to develop and procure the ASP was not

---

<sup>22</sup>GAO, *Supply Chain Security: CBP Needs to Conduct Regular Assessments of Its Cargo Targeting System*, GAO-13-9 (Washington, D.C.: Oct. 25, 2012).

<sup>23</sup>GAO, *Combating Nuclear Smuggling: Lessons Learned from Cancelled Radiation Portal Monitor Program Could Help Future Acquisitions*, GAO-13-256 (Washington, D.C.: May 13, 2013). As we reported in 2013, ASP may have reduced the rate of alarms that are triggered by benign radioactive materials that naturally occur in common items such as kitty litter and granite. The reduced rate of alarms may also have reduced the number of unnecessary secondary screenings.

---

rigorous enough.<sup>24</sup> Once the testing became more rigorous, these portals did not perform well enough to warrant deployment. Accordingly, DHS scaled back the program in 2010 and subsequently canceled the program in 2012, after DNDO had spent more than \$280 million on development and testing.

- **CSI program overseas:** CBP has also developed the Container Security Initiative (CSI) program, which places CBP officials at selected foreign ports to use intelligence and risk assessment information to work with host country officials to determine whether U.S.-bound cargo container shipments from those ports are at risk of containing WMDs or other terrorist contraband.<sup>25</sup> CBP's selection of the initial 23 CSI ports in 2002 was primarily based on the volume of U.S.-bound containers, but beginning in 2003, CBP considered more threat information when it expanded the number of CSI ports. In September 2013, we reported that CBP had not assessed the risk posed by foreign ports that ship cargo to the United States since 2005 and recommended that DHS direct CBP to periodically assess the risks from all foreign ports that ship cargo to the United States and use the results of these risk assessments to inform any future adjustments to CSI locations.<sup>26</sup> DHS concurred and reported that, by December 2014, it plans to develop a process for conducting such periodic risk assessments. In addition, in a May 2014 letter to Congress, the Secretary of Homeland Security reported that DHS will work to increase the percentage of containers scanned abroad and will engage other countries to discuss the potential expansion of CSI to additional ports that ship high-risk cargo to the United States.
- **Megaports Initiative:** We reported in 2005 and 2012 on the Megaports Initiative—a National Nuclear Security Administration (NNSA) nonproliferation program that funds the installation of radiation detection

---

<sup>24</sup>For further information regarding our work on the advanced spectroscopic portal, see GAO, *Combating Nuclear Smuggling: Additional Actions Needed to Ensure Adequate Testing of Next Generation Radiation Detection Equipment*, GAO-07-1247T (Washington, D.C.: Sept. 18, 2007); and *Combating Nuclear Smuggling: DHS Improved Testing of Advanced Radiation Detection Portal Monitors, but Preliminary Results Show Limits of the New Technology*, GAO-09-655 (Washington, D.C.: May 29, 2009).

<sup>25</sup>As of July 2013, there were 58 CSI ports in 32 countries that, collectively, accounted for over 80 percent of the container shipments imported into the United States.

<sup>26</sup>GAO, *Supply Chain Security: DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports*, GAO-13-764 (Washington, D.C.: Sept. 16, 2013).

---

equipment at seaports overseas.<sup>27</sup> The Initiative seeks to deter, detect, and interdict nuclear or other radiological materials from being smuggled through foreign seaports. At the time of our 2012 report, NNSA had completed 42 of 100 planned Megaports in 31 countries. NNSA equipped these seaports with radiation detection equipment and established training programs for foreign personnel. However, in 2012, we found that the Megaports Initiative and DHS's Container Security Initiative were not sufficiently coordinated. For example, in two countries where both programs were operating, DHS officials told us that they were using personal radiation detectors—a type of equipment intended for personal safety but not appropriate for scanning containers—to inspect containers if their radiation detection equipment was broken. In both countries, the Megaports Initiative had more suitable equipment that DHS officials could have used to improve detection capabilities. We made several recommendations in our 2012 report, including that NNSA and DHS jointly assess the extent to which the two initiatives are effectively coordinated. In response to this recommendation, in December 2012, NNSA established standard operating procedures that formalized coordination between the two programs. Subsequently, the administration concluded that there were diminishing returns for new Megaports and limitations in the effectiveness of the technologies used and proposed reducing the initiative's fiscal year 2013 budget by about 85 percent. As a result, NNSA had planned to shift the initiative's focus from establishing new Megaports to sustaining existing ones. However, we reported in 2012 that NNSA had not finalized a long-term plan for ensuring the sustainability of Megaports operations and recommended that NNSA finalize this plan. In response to this recommendation, in October 2012, NNSA finalized its sustainability plan.

- **Secure Freight Initiative:** The Secure Freight Initiative (SFI) established pilot projects to test the feasibility of scanning 100 percent of U.S.-bound containers at foreign ports to address concerns that terrorists would smuggle WMDs inside cargo containers bound for the United States. We testified in June 2008 that CBP faced difficulties in implementing SFI because of challenges related to host nation examination practices, performance measures, resource constraints, logistics, and technology

---

<sup>27</sup>See GAO, *Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports*, GAO-05-375 (Washington, D.C.: Mar. 31, 2005) and *Combating Nuclear Smuggling: Megaports Initiative Faces Funding and Sustainability Challenges*, GAO-13-37 (Washington, D.C.: Oct. 31, 2012).

---

limitations.<sup>28</sup> In October 2009, we issued a report on SFI and recommended, among other things, that DHS, in consultation with the Secretaries of Energy and State, conduct cost-benefit and feasibility analyses and provide the results to Congress. CBP partially concurred with these recommendations, but CBP officials told us that CBP does not plan to conduct the analyses because it has insufficient funds to conduct such analyses. The SAFE Port Act, as amended in 2007 by the Implementing Recommendations of the 9/11 Commission Act, directed DHS to implement 100 percent scanning of U.S.-bound maritime cargo container shipments by July 2012, but authorized DHS to extend the deadline for 2 years and renew such extension in additional 2-year increments if at least two of six statutory conditions existed.<sup>29</sup> The former DHS Secretary exercised this authority and formally notified Congress by letter dated May 2, 2012 that she had extended the deadline until July 1, 2014. In a letter to Members of Congress, in May 2014, the Secretary of Homeland Security stated that the conditions and supporting evidence cited in the 2012 deadline extension—negative effects on trade capacity and the flow of cargo and characteristics of foreign ports that prevent the installation of scanning systems—continue to prevail and preclude full-scale implementation.

- **Partnerships with industry:** The Customs-Trade Partnership Against Terrorism (C-TPAT) program is a voluntary program that enables CBP officials to work in partnership with private companies to review and approve the security of their international supply chains. Companies that join the C-TPAT program commit to improving the security of their supply chains and agree to allow CBP to verify, among other things, that their security measures meet or exceed CBP's minimum security requirements. This allows CBP to ensure that the security measures outlined in a member's security profile are in place and effective. In return for their participation in the program, C-TPAT members are entitled to a reduced likelihood of scrutiny of their cargo. In April 2008, we found that the C-TPAT program held promise as part of CBP's multifaceted maritime security strategy.<sup>30</sup> We also found that the program allows CBP

---

<sup>28</sup>GAO, *Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers*, GAO-08-533T (Washington, D.C.: June 12, 2008).

<sup>29</sup>Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (amending 6 U.S.C. § 982(b)).

<sup>30</sup>GAO, *Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices*, GAO-08-240 (Washington, D.C.: Apr. 25, 2008).

---

to develop partnerships with the international trade community and provides CBP with a level of information sharing that would otherwise not be available due to CBP's usual jurisdiction and activities. However, our report raised questions about the management of the program's records and performance, and challenges in verifying that C-TPAT members meet security criteria. Thus, we recommended in 2008 that CBP strengthen program management by developing planning documents and performance measures, and by improving the process for validating security practices of C-TPAT members. CBP agreed with these recommendations and, in 2009, completed its development of policies, performance measures and guidance to ensure process improvements.

- **International Port Security program:** While CBP is focused on the security of the cargo shipped to the United States from foreign ports, the Coast Guard is focused on the security of both foreign and U.S. ports, and the vessels arriving in U.S. ports. Under the International Port Security program, Coast Guard officials visit foreign ports to evaluate their antiterrorism security measures against established international standards. We reported in October 2007 that the Coast Guard had visited over 100 countries and found that most had substantially implemented international standards.<sup>31</sup> In September 2012, we reported that the Coast Guard had made progress with implementing its International Port Security program despite a number of challenges.<sup>32</sup> For example, we reported that the Coast Guard was able to alleviate sovereignty concerns of some countries by inviting foreign delegations to visit U.S. ports. Further, as we reported in September 2013, the Coast Guard had visited port facilities in over 150 countries by June of 2013 and developed a risk-informed model—that it updates annually—as part of its International Port Security program.<sup>33</sup> The Coast Guard uses the model to make informed decisions on how to engage each country within the International Port Security program, including (1) how often to visit ports, (2) how many staff to assign to a particular visit, and (3) whether the country requires assistance to enhance its port security.

---

<sup>31</sup>GAO, *Maritime Security: The SAFE Port Act: Status and Implementation One Year Later*, GAO-08-126T (Washington, D.C.: Oct. 30, 2007).

<sup>32</sup>GAO, *Maritime Security: Progress and Challenges 10 Years after the Maritime Transportation Security Act*, GAO-12-1009T (Washington, D.C.: Sept. 11, 2012).

<sup>33</sup>GAO-13-764.

- 
- **Mutual recognition:** Through mutual recognition arrangements with foreign partners, the security-related practices and programs established by the customs or maritime security administration of one partner are recognized and accepted by the administration of another.<sup>34</sup> Both CBP and the Coast Guard have entered into such arrangements. For example, CBP can expand the reach of its supply chain security programs (such as C-TPAT) through mutual recognition arrangements. According to the World Customs Organization, mutual recognition arrangements allow customs administrations to target high-risk shipments more effectively and expedite low-risk shipments by, for example, reducing redundant examinations.<sup>35</sup> In September 2013, we found that mutual recognition arrangements may allow the Coast Guard to allocate resources more efficiently and reduce risks.<sup>36</sup> For example, we reported that the Coast Guard signed a memorandum of understanding with the European Union that establishes a process for mutually recognizing security inspections of each other's ports.<sup>37</sup> According to DHS documents and Coast Guard officials in Europe, by signing this memorandum of understanding, the Coast Guard plans to reassign some International Port Security officials from Europe to Africa, where certain countries are having more difficulties than others in implementing effective antiterrorism measures in their ports. Further, we reported that one trade-off of signing the memorandum of understanding is that Coast Guard's International Port Security officials will not have the same opportunities to have face-to-face interactions and share port security information and practices directly with their European Union counterparts as in the past. Despite this trade-off, Coast Guard officials stated that entering into such arrangements increases efficiencies and noted that they intend to negotiate additional

---

<sup>34</sup>Mutual recognition arrangements can be entered into with other countries as well as other governing bodies, such as the European Union. For the purposes of this testimony, the countries and governing bodies that enter into mutual recognition arrangements with the United States are considered partners.

<sup>35</sup>The World Customs Organization is an intergovernmental organization representing the customs administrations of 179 countries, which aims to enhance the effectiveness and efficiency of Customs administrations.

<sup>36</sup>GAO-13-764.

<sup>37</sup>According to DHS officials, the European Union characterizes its port visits as "inspections." Under the memorandum of understanding procedures, the Coast Guard recognizes a successful European Union inspection of its member states' ports in the same manner as it would recognize a successful country visit by Coast Guard inspectors. Coast Guard officials stated that they have collaborated with their European counterparts to develop standard operating procedures for these port inspections.

---

memorandums of understanding with other foreign governments that have strong port inspection programs.

---

Thank you Chairman Carper, Ranking Member Coburn, and Members of the Committee. This completes my prepared statement. I would be happy to respond to any questions you may have at this time.



---

September 2013

## SUPPLY CHAIN SECURITY

### DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports

## GAO Highlights

Highlights of GAO-13-704, a report to congressional committees

### Why GAO Did This Study

Foreign ports and the cargo carried by vessels from these ports are critical to the U.S. economy, but can be disrupted by terrorism. While DHS, CBP and the Coast Guard are responsible for maritime security, through CSI, CBP identifies and examines U.S.-bound cargo that may conceal WMD, and through C-TPAT, CBP partners with international trade community members to secure the flow of U.S.-bound goods. Under the IPS program, Coast Guard officials visit foreign ports to assess compliance with security standards. GAO was asked to review DHS's maritime security programs. This report addresses (1) the extent to which DHS has assessed the foreign ports that pose the greatest risk to the global supply chain and focused its maritime container security programs to address those risks, and (2) whether DHS has taken steps to help ensure the efficiency and effectiveness of its maritime security programs. GAO analyzed DHS risk models and maritime security program strategies, met with program officials, and visited six foreign countries selected on the basis of participation in CSI, varied cargo shipment risk levels, and other factors.

### What GAO Recommends

GAO recommends that CBP periodically assess the supply chain security risks from foreign ports that ship cargo to the United States and use the results to inform any future expansion of CSI and determine whether changes need to be made to existing CSI ports. DHS concurred with GAO's recommendation.

View GAO-13-704. For more information, contact Stephen Lathrop at (301) 512-3810 or [slathrop@gao.gov](mailto:slathrop@gao.gov).

September 2013

## SUPPLY CHAIN SECURITY

### DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports

### What GAO Found

Department of Homeland Security (DHS) components have developed models to assess the risks of foreign ports and cargo, but not all components have applied risk management principles to assess whether maritime security programs cover the riskiest ports. The U.S. Coast Guard uses its risk model to inform operational decisions for its International Port Security (IPS) program and annually updates its assessment. In contrast, U.S. Customs and Border Protection (CBP) has not regularly assessed ports for risks to cargo under its Container Security Initiative (CSI) program. CBP's selection of the initial 23 CSI ports was primarily based on the volume of U.S.-bound containers, but beginning in 2003, CBP considered more threat information when it expanded the number of CSI ports. CBP has not assessed the risk posed by foreign ports that ship cargo to the United States for its CSI program since 2005. In 2009, CBP developed a model that ranked 356 potential expansion ports for a related program on the basis of risk, but it was never implemented because of budget cuts. By applying CBP's risk model to fiscal year 2012 cargo shipment data, GAO found that CSI did not have a presence at about half of the ports CBP considered high risk, and about one fifth of the existing CSI ports were at lower risk locations. Since the CSI program depends on cooperation from sovereign host countries, there are challenges to implementing CSI in new foreign locations, and CBP's negotiations with other countries have not always succeeded. For example, CBP officials said it is difficult to close CSI ports and open new ports because removing CSI from a country might negatively affect U.S. relations with the host government. However, periodically assessing the risk level of cargo shipped from foreign ports and using the results to inform any future expansion of CSI to additional locations, as well as determine whether changes need to be made to existing CSI ports, would help ensure that CBP is allocating its resources to provide the greatest possible coverage of high-risk cargo to best mitigate the risk of importing weapons of mass destruction (WMD) or other terrorist contraband into the United States through the maritime supply chain.

DHS has taken steps to improve the efficiency and effectiveness of its maritime security programs, but faces host country political and legal constraints. The Coast Guard has implemented a risk-informed model that prioritizes the countries to visit and assist. Also, the Coast Guard and CBP have made arrangements with foreign government entities to mutually recognize inspections of each other's ports and maritime supply chains through the IPS and Customs-Trade Partnership Against Terrorism (C-TPAT) programs. CBP has also utilized technological improvements to target some U.S.-bound cargo shipments remotely from the United States to reduce CSI staff in foreign countries. However, CBP faces political and legal constraints in host countries. For example, according to CBP and government officials in one country, a national law precludes the transmission of electronic scanned images other than to host government Customs officials. As a result, CSI officials must be present at each CSI port in that country to view the scanned images. Further, in some ports, CBP has made efforts to expand the scope of its CSI targeting to include contraband other than WMD, but that is subject to approval by the host governments.

---

## Contents

Letter		1
	Background	7
	DHS Has Developed Models to Assess Foreign Port Risks, but CBP Has Not Assessed Whether Its CSI Locations Remain Valid	16
	DHS Has Taken Steps to Improve the Efficiency and Effectiveness of Its Maritime Container Security Programs, but Faces Constraints	24
	Conclusions	37
	Recommendations for Executive Action	37
	Agency Comments and Our Evaluation	38
Appendix I	Information on Foreign Ports That Coordinate Maritime Cargo Container Security Efforts with U.S. Customs and Border Protection	39
Appendix II	Comments from the Department of Homeland Security	42
Appendix III	GAO Contact and Staff Acknowledgments	44
Related GAO Products		45
Tables		
	Table 1: Coast Guard International Port Security Program Visits, by Country Risk Level, for Fiscal Year 2012	26
	Table 2: Foreign Ports That CBP Coordinates with Regarding Maritime Container Shipment Examinations, as of July 2013 (Listed by Date Port Began CSI Operations)	39
Figures		
	Figure 1: Illustrative Example of Key Points in the Global Supply Chain	8
	Figure 2: Department of Homeland Security's (DHS) Key Maritime Security Programs	9

---

Figure 3: Panama Customs Examining a Container Using Imaging Equipment, Port of Balboa, Panama	11
Figure 4: Partial View of the Port of Singapore	19
Figure 5: Map Showing the Variety of Targeting Approaches Customs and Border Protection Uses in Container Security Initiative Countries as of July 2013	33

---

**Abbreviations**

AEO	authorized economic operator
ATS	Automated Targeting System
CBP	U.S. Customs and Border Protection
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
DHS	Department of Homeland Security
DOE	Department of Energy
IPS	International Port Security program
ISPS Code	International Ship and Port Facility Security Code
MOU	memorandum of understanding
MRA	mutual recognition arrangement
MTSA	Maritime Transportation Security Act
NTC-C	National Targeting Center-Cargo
SAFE Port Act	Security and Accountability for Every Port Act
WMD	weapons of mass destruction

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



September 16, 2013

The Honorable Thomas R. Carper  
Chairman  
The Honorable Tom Coburn  
Ranking Member  
Committee on Homeland Security and Governmental Affairs  
United States Senate

The Honorable Susan M. Collins  
United States Senate

Foreign ports and the cargo carried by vessels from these ports are critical to the U.S. economy but can also be exploited by terrorists. According to the U.S. Department of Transportation, the majority of U.S. imports arrive by ocean vessel, and much of that is transported in cargo containers.<sup>1</sup> Cargo containers are an important segment of the global supply chain—the flow of goods from manufacturers to retailers—and can present significant security concerns. For example, a 2012 risk assessment by the Department of Homeland Security (DHS) found that attacks could cause major disruptions to the maritime supply chain. DHS officials believe that the likelihood of terrorists smuggling weapons of mass destruction (WMD) into the United States in cargo containers is relatively low; however, the consequences of such an event could be catastrophic. Although there have been no known incidents of cargo containers being used to transport WMD, ensuring the security of cargo containers remains an important role for the federal government given that criminals have exploited containers for other illegal purposes, such as smuggling weapons, people, and illicit substances. To balance the government's need to help secure the global supply chain while also promoting the efficient and secure movement of goods, the White House issued the National Strategy for Global Supply Chain Security in January 2012, which emphasizes a risk-informed approach for DHS's cargo security programs across all modes of transportation.<sup>2</sup> This strategy

<sup>1</sup>U.S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics, *America's Container Ports: Linking Markets at Home and Abroad* (Washington, D.C.: January 2011).

<sup>2</sup>The White House, *National Strategy for Global Supply Chain Security* (Washington, D.C.: January 2012).

---

builds on a number of strategic efforts to strengthen the global supply chain.<sup>3</sup> While DHS' cargo security programs cover all modes of transportation, the focus of this report is on DHS's maritime security programs.

In the federal government, U.S. Customs and Border Protection (CBP) and the Coast Guard, both within DHS, are two key agencies responsible for maritime security issues. In particular, CBP is responsible for, among other things, assessing the overall security of the supply chain and reducing the vulnerabilities associated with U.S.-bound cargo container shipments; and the Coast Guard is responsible for, among other things, assessing the effectiveness of security measures in foreign ports and vessels that trade with the United States.

In performing its container security responsibilities, CBP has developed a layered, risk management approach<sup>4</sup> that includes two security programs—the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT) program. Under the CSI program, CBP places officials (targeters) at select foreign seaports to use intelligence and risk assessment information to determine whether U.S.-bound cargo container shipments from those ports are at risk of containing WMD or other terrorist contraband. To aid in this process, CBP targeters use the Automated Targeting System (ATS)—an enforcement and decision support system that incorporates a set of rules to assess information provided by supply chain parties, such as importers—to identify high-risk shipments. C-TPAT is a voluntary program in which CBP officials work with private companies, referred to as partners, to review the security of their international supply chains and improve the security of their shipments to the United States. In return, C-TPAT partners receive various incentives to facilitate the flow of legitimate cargo, such as reduced scrutiny of their shipments.

---

<sup>3</sup>See, for example, the *National Strategy to Combat Weapons of Mass Destruction* (Washington, D.C.: December 2002), the *National Strategy for Maritime Security* (Washington, D.C.: September 2005), the *Strategy to Enhance International Supply Chain Security* (Washington, D.C.: 2007), the *National Security Strategy* (May 2010), the *National Strategy for Counterterrorism* (Washington, D.C.: June 2011), and the *National Strategy to Combat Transnational Organized Crime* (Washington, D.C.: July 2011).

<sup>4</sup>Risk management is a strategy called for by federal law and presidential directive and is meant to help policy makers and program officials most effectively mitigate risk while allocating limited resources under conditions of uncertainty.

---

In addition to the CBP container security programs, the Coast Guard operates the International Port Security (IPS) program in which Coast Guard officials, in conjunction with foreign officials, visit and assess the implementation of security measures in foreign ports against established, international port security standards to help ensure the security of maritime commerce. In addition, CBP and the Coast Guard have separately entered into arrangements with foreign counterpart agencies to validate and mutually recognize each others' port security practices to more efficiently address maritime and supply chain security.

Since September 11, 2001, Congress has passed various laws to address concerns about the security of maritime cargo container shipments in the global supply chain. The Maritime Transportation Security Act of 2002 (MTSA)<sup>5</sup> called for the establishment of a program to evaluate and certify secure systems of international transportation, including standards and procedures for screening and evaluating cargo containers prior to loading them onto vessels and for securing and monitoring cargo while in transit.<sup>6</sup> One MTSA provision requires DHS to assess the effectiveness of the antiterrorism measures maintained at ports from which foreign vessels depart to the United States, or in any other port the Secretary of Homeland Security believes may pose a risk to international maritime commerce.<sup>7</sup> The Secretary delegated this responsibility to the Coast Guard, which initiated IPS in 2004 to carry out this responsibility. To further address container security concerns, Congress passed, and the President signed, the Security and Accountability for Every (SAFE) Port Act in 2006, which included provisions that codified the CSI and C-TPAT programs.<sup>8</sup>

Given the importance of maritime transportation to the economy, the wide spectrum of security threats, and the constrained budget environment, you asked that we review DHS's maritime supply chain security programs. In particular, this report addresses the following questions:

---

<sup>5</sup>Pub. L. No. 107-295, 116 Stat. 2064.

<sup>6</sup>See 46 U.S.C. § 70116.

<sup>7</sup>46 U.S.C. § 70108.

<sup>8</sup>Pub. L. No. 109-347, 120 Stat. 1884.

- 
- To what extent has DHS assessed the risks to the global supply chain associated with foreign ports and focused its maritime security programs to address those risks?
  - What actions has DHS taken to help ensure the efficiency and effectiveness of its maritime supply chain security programs?

To address the first question, we identified how DHS's components assess risk to the supply chain associated with foreign ports and countries.<sup>9</sup> Specifically, we (1) gathered information on the criteria used to determine high-risk locations and the key stakeholders involved in developing any models or methodologies used to do so, (2) reviewed the methodology used to construct any models, and (3) determined the sufficiency of the models to identify high-risk locations. In particular, we reviewed the Coast Guard's IPS model for determining operational decisions, the methodology CBP used to select CSI ports, and the model developed by CBP and the Department of Energy (DOE) for potentially expanding cargo-scanning operations at foreign ports. To the extent possible, we compared the relative risk of foreign ports generated by these models with the location of CSI ports to determine the degree of correlation. As part of this process, we combined fiscal year 2012 data on the number of U.S.-bound shipments from foreign ports with data from the models and narrowed the list of ports based on a minimum of 1,000 U.S.-bound shipments—a step CBP took when developing its model in conjunction with DOE. We assessed the reliability of the models by interviewing staff responsible for development of the methodologies and the data and reviewing documentation related to the development, application, and reviews of the models. We concluded that the models and data were sufficiently reliable for the purposes of our review. In addition, we interviewed CBP, Coast Guard, DOE, and Department of State officials about the process used for identifying high-risk locations, the stakeholders involved in this process, and the status of these efforts. We compared this information with SAFE Port Act requirements, key elements for a risk management approach,<sup>10</sup> and the principles laid out in

---

<sup>9</sup>For the purposes of this report, we used the following DHS definition of risk: the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. For example, risk is the expected consequences associated with a terrorist organization smuggling a WMD into a container at a foreign port and detonating that weapon in the United States.

<sup>10</sup>These key elements are contained in DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009).

---

the *National Strategy for Global Supply Chain Security*. We also reviewed our prior work on risk management practices and compared our analysis of CBP's actions with those practices.<sup>11</sup>

To address the second question, we focused primarily on the CSI, C-TPAT, and IPS programs. Specifically, we analyzed CBP efforts to implement the fiscal year 2012 through 2017 CBP Office of Field Operations Strategic Plan and associated strategies in the CSI and C-TPAT Strategy Action Plans. We reviewed DHS documentation, such as the 2013 *DHS Annual Performance Report* and budget documents. Further, we reviewed CSI and C-TPAT performance measurement data and analyzed CSI staffing data from fiscal years 2009 through fiscal years 2012—the 4 most recent years for which data were available—to review the extent to which CSI staffing models have increased efficiency. In addition, we analyzed fiscal year 2012 Coast Guard foreign port visit data and foreign country risk data to determine the extent to which the Coast Guard uses the results of its risk assessments to help determine the amount of resources needed when visiting foreign countries' ports. We reviewed documentation related to the data sources, such as the 2013 *DHS Annual Performance Report*, and obtained written responses from knowledgeable agency officials regarding any issues with completeness, accuracy, and management of the data. We determined that these CBP and Coast Guard data were sufficiently reliable for the purposes of our review. We visited six geographically dispersed foreign countries that participate in the CSI program—two each in Latin America (Panama and Argentina), Asia (Japan and Singapore), and Europe (the Netherlands and England)—that also provided a range of coverage regarding (1) cargo container shipment risk levels, (2) volume of cargo containers shipped to the United States, (3) the proportion of transshipped containers,<sup>12</sup> and (4) participation in mutual recognition arrangements (MRA) with CBP or the Coast Guard.<sup>13</sup> We interviewed DHS, Department

---

<sup>11</sup>GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005). Our prior work identified a risk management framework that we used to evaluate activities related to homeland security and combating terrorism.

<sup>12</sup>Transshipped containers are those that are unloaded from vessels at ports and are then reloaded to different vessels.

<sup>13</sup>Through MRAs with other partners, the security-related practices and programs taken by the customs or maritime security administration of one country are recognized and accepted by the administration of another. These arrangements are discussed in more detail later in this report.

---

of State, and foreign government officials in the countries we visited, and also met with other maritime supply chain stakeholders, such as officials from private industry and the World Customs Organization, to discuss implementation of DHS's maritime security programs, how these programs are integrated, the specific maritime security threats each program targets, and the impact of these programs on the security of U.S.-bound cargo container shipments. We worked with relevant officials at the U.S. embassies in the foreign countries we visited to help us determine which foreign government and industry officials to interview. The results from our visits to these six countries cannot be generalized; however, the visits provided us with first-hand observations on cargo security screening and targeting practices at the ports visited, and insights regarding how DHS implements its overseas maritime container security programs and the impact of these programs. In addition, we contacted officials from the seven partners that have signed an MRA with CBP and obtained the views of cognizant officials representing four of these partners. While the results of these meetings cannot be generalized to all seven MRA-signatory partners, they provided insights regarding the impact of the MRAs on DHS and other maritime security programs. Further, we interviewed the DHS Acting Director of Transportation & Cargo, Transborder Policy, to discuss implementation of the *National Strategy for Global Supply Chain Security* and how it affects maritime container security programs. We also interviewed Coast Guard officials responsible for the IPS program to discuss development and implementation of the Coast Guard IPS risk model and mutual recognition efforts.<sup>14</sup>

We conducted this performance audit from October 2012 to September 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

---

<sup>14</sup>We also interviewed U.S. Immigration and Customs Enforcement officials regarding the Global Shield initiative to stem the illegal flow of precursor chemicals used in improvised explosive devices (IED), but we determined this program was outside the scope of this review because it is an international initiative, not a U.S. maritime security program. Global Shield is a World Customs Organization initiative in collaboration with the United Nations Office on Drugs and Crime and Interpol. Since its initiation in October 2010, more than 80 participating countries have monitored the import and export of 14 explosive precursor chemicals—identified as those most prevalently used in IEDs—around the world, in order to secure the global supply chain.

---

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

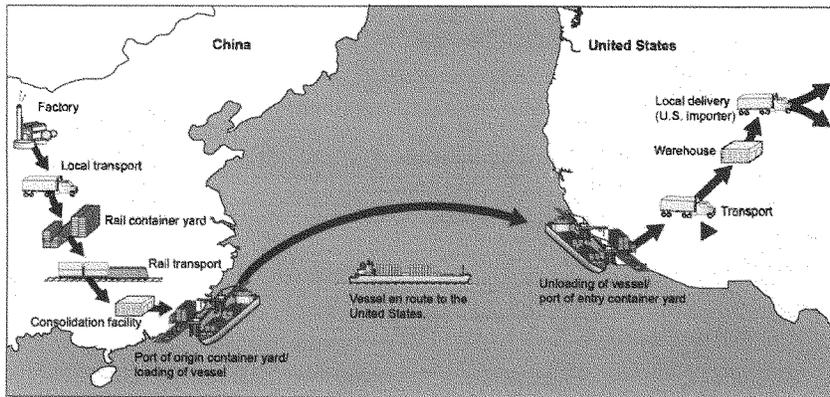
---

## Background

### Vulnerabilities of Maritime Cargo Containers in the Global Supply Chain

Ports are critical gateways for the movement of commerce through the global supply chain. According to CBP data, in fiscal year 2012, about 11.5 million cargo container shipments arrived from more than 650 foreign ports—meaning roughly 31,000 maritime container shipments arrived each day that year. The facilities, vessels, and infrastructure within ports, and the cargo passing through them, all have vulnerabilities that terrorists could exploit. Every time responsibility for cargo in containers changes hands along the supply chain there is the potential for a security breach. While there have been no known incidents of containers being used to transport WMDs, criminals have exploited containers for other illegal purposes, such as smuggling weapons, people, and illicit substances. Figure 1 illustrates the notional key points of transfer involved in the global supply chain—from the time that a container is loaded with goods at a foreign factory to its arrival at the U.S. seaport and ultimately the U.S. importer.

Figure 1: Illustrative Example of Key Points in the Global Supply Chain

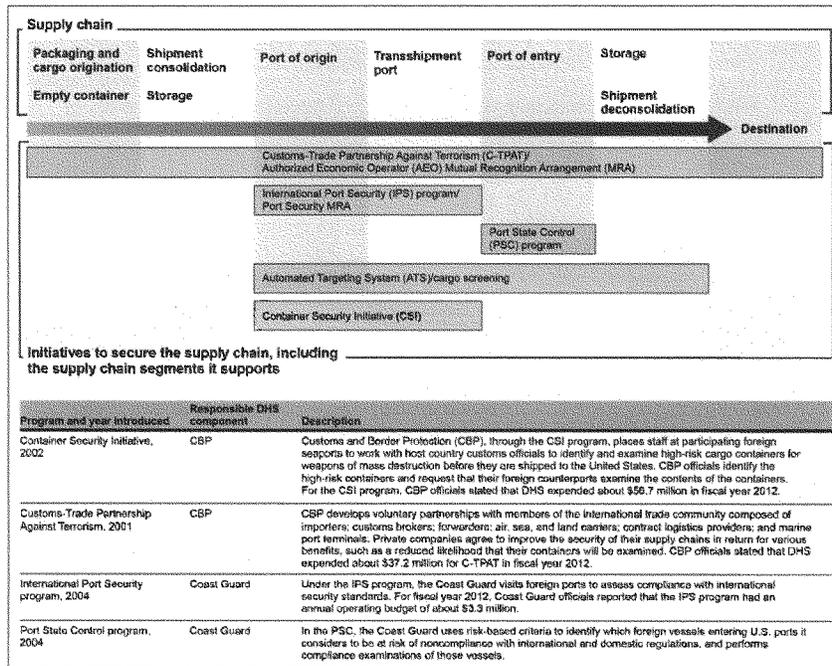


Source: GAO. Map Resources (map).

**DHS Efforts to Secure the Global Supply Chain**

DHS has taken steps to secure the global supply chain, including the cargo in oceangoing containers destined for the United States. DHS's strategy includes focusing security efforts beyond U.S. borders to target and examine high-risk cargo and vessels before they enter U.S. seaports. DHS's strategy is based on a layered approach of related programs that attempt to focus resources on potentially risky foreign ports, vessels, and cargo container shipments while allowing other cargo container shipments to proceed without unduly disrupting the flow of commerce into the United States. DHS's maritime security programs support the *National Strategy for Global Supply Chain Security*, which emphasizes risk management and coordinated engagement with key stakeholders who also have supply chain roles and responsibilities. Figure 2 shows DHS's key maritime security programs and the various segments in the global supply chain where these programs are focused.

Figure 2: Department of Homeland Security's (DHS) Key Maritime Security Programs



Source: GAO analysis of information provided by DHS.

Notes: AEOs include, for example, manufacturers, importers, exporters, brokers, ports, airports, terminal operators, warehouses, and distributors.

Through MRAs with other partners, the security-related practices and programs taken by the Customs or maritime security administration of one country are recognized and accepted by the administration of another.

ATS is a CBP enforcement and decision support system that incorporates a set of rules to assess information provided by supply chain parties, such as importers, to identify high risk shipments.

---

**Container Security Initiative**

CSI is a program that aims to identify and examine U.S.-bound cargo container shipments that could pose a high risk of concealing WMDs or other terrorist contraband by reviewing advanced cargo information about the shipments. As part of the CSI program, CBP officers are stationed at select foreign seaports to identify high-risk U.S.-bound container cargo shipments before they are loaded onto U.S.-bound vessels. As of July 2013, there were 58 CSI ports in 32 countries that, collectively, account for over 80 percent of the container shipments imported into the United States. In addition to the CSI ports where CBP placed targeters, CBP also entered into arrangements with Australia and New Zealand to remotely target U.S.-bound cargo container shipments from the United States.<sup>15</sup> A complete listing of the countries that participate in the CSI program can be found in appendix I.

CBP officers stationed at foreign CSI ports are to conduct the following activities:

- **Target U.S.-bound container shipments.** As we previously reported, CBP targeters use ATS and other information to electronically review information about U.S.-bound shipments departing from the foreign port—a process CBP refers to as screening.<sup>16</sup> CBP targeters review the ATS risk scores and additional information to identify high-risk shipments with a potential nexus to terrorism—a process referred to as targeting. The CBP targeters make a final determination about which containers are high risk and will be referred to host government officials for examination.
- **Request examinations of high-risk container shipments.** According to our work and updates provided by CBP officials, CBP

---

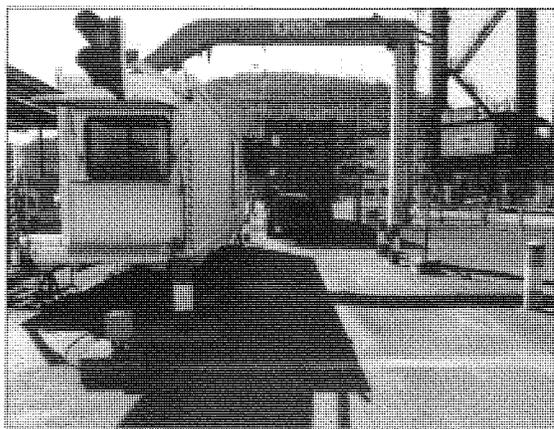
<sup>15</sup>According to CBP officials, CBP entered into arrangements with New Zealand (April 2006) and Australia (November 2011) to remotely target U.S.-bound cargo container shipments from Auckland and Melbourne, respectively. Further, in August 2007, CBP began targeting containers at Shenzhen, China, that did not originally participate in CSI. According to CBP officials, CSI targeters in Shenzhen are also able to review and target shipments from Shekou, China, and can drive to that port to witness examinations. For the purposes of this report, we consider a port to be a CSI port if CBP has entered into an arrangement or otherwise coordinates with a foreign country to target U.S.-bound cargo container shipments from that port. Accordingly, we consider the number of CSI ports to be 61 rather than 58. Appendix I provides a complete listing of the 61 CSI ports.

<sup>16</sup>GAO, *Supply Chain Security: CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain*, GAO-08-538 (Washington, D.C.: Aug. 15, 2008).

---

targeters work with host country government officials to mitigate high-risk container shipments.<sup>17</sup> Actions may include resolving discrepancies in shipment information, scanning cargo containers' contents with radiation detection or imaging equipment (as shown in fig. 3), or conducting physical inspections of the containers' contents.

**Figure 3: Panama Customs Examining a Container Using Imaging Equipment, Port of Balboa, Panama**



Source: GAO.

#### Customs-Trade Partnership Against Terrorism

According to our prior work and updates provided by CBP officials, C-TPAT aims to secure the flow of goods bound for the United States by developing a voluntary public-private sector partnership with stakeholders of the international trade community.<sup>18</sup> C-TPAT partners agree to adhere

---

<sup>17</sup>GAO-08-538.

<sup>18</sup>GAO-08-538.

---

International Port Security Program	<p>to the program's eight established minimum security criteria in areas such as physical security, personnel security, and information technology. C-TPAT partners also agree to provide CBP with information regarding their security processes and procedures and allow CBP to validate or verify that these security measures are in place. In return, C-TPAT partners receive various incentives, such as reduced examinations based upon lower risk scores.</p> <p>In addition to the CBP programs, the Coast Guard also has an internationally focused maritime security program, the IPS program. Under the IPS program, Coast Guard officials visit foreign ports to evaluate their antiterrorism security measures against established International Ship and Port Facility Security (ISPS) Code standards.<sup>19</sup> In addition, the Coast Guard collects and shares best practices with foreign countries and engages in efforts to help facilitate a comprehensive and consistent approach to maritime security in ports worldwide. Coast Guard officials reported that from its inception in April 2004 through June 2013, IPS program officials have visited port facilities in 151 countries and overseas protectorates engaged in maritime trade with the United States. According to its visits and the information provided by the foreign countries as part of those visits, the Coast Guard determines whether the countries have effectively implemented the ISPS Code and are maintaining effective security measures in their ports. If the Coast Guard finds that a country is not maintaining port security measures, the Coast Guard can impose conditions of entry on vessels arriving at the United States from that country.<sup>20</sup></p>
Port State Control Program	<p>The Coast Guard uses the results of the port risk assessments to help decide which foreign vessels to board or inspect through its Port State Control program, according to the U.S. Coast Guard <i>International Port</i></p>

---

<sup>19</sup>The IPS program uses the ISPS Code as the benchmark by which it measures the effectiveness of a country's antiterrorism measures in a port. The code was developed after the September 11, 2001, terrorist attacks to establish measures to enhance the security of ships and port facilities with a standardized and consistent security framework. The ISPS Code requires facilities to conduct an assessment to identify threats and vulnerabilities and then develop security plans based on the assessment. The requirements of this code are performance-based; therefore, compliance can be achieved through a variety of security measures.

<sup>20</sup>Conditions of entry may include restricting a vessel's movement within U.S. ports or requiring the vessel to take additional security measures, such as stationing guards at each access point of the ship when in a U.S. port.

Mutual Recognition  
Arrangements

*Security Program: Annual Report 2012.*<sup>21</sup> While the Port State Control program does not directly affect container security, as part of this program, the Coast Guard uses risk-based criteria to identify which foreign vessels entering U.S. ports and waterways it considers to be at risk of noncompliance with international or domestic regulations, and performs compliance examinations of these vessels. The risk-based criteria include the vessel's management, the flag state that the vessel is registered under, the vessel's recognized security organization, and the vessel's security compliance history resulting from previous examinations.

Through mutual recognition arrangements with foreign partners, the security-related practices and programs taken by the Customs or maritime security administration of one partner are recognized and accepted by the administration of another.<sup>22</sup> Both CBP and the Coast Guard have entered into such arrangements. For example, CBP can expand the reach of its supply chain security programs through MRAs. According to the World Customs Organization, mutual recognition allows Customs administrations to target high-risk shipments more effectively and expedite low-risk shipments by, for example, reducing redundant examinations.<sup>23</sup> The World Customs Organization distinguishes between mutual recognition of Customs controls and mutual recognition of authorized economic operator (AEO) programs.<sup>24</sup>

- **Mutual recognition of Customs controls (Customs-to-Customs MRAs):** This is achieved when, for example, the Customs administrations of two countries have confidence in and accept each other's procedures for targeting and inspecting cargo shipped in containers.

<sup>21</sup>U.S. Coast Guard, *International Port Security Program: Annual Report 2012* (Washington, D.C.: March 31, 2012).

<sup>22</sup>MRAs can be entered into with other countries as well as other governing bodies, such as the European Union. For the purposes of this report, the countries and governing bodies that enter into MRAs with the United States are considered "partners."

<sup>23</sup>The World Customs Organization is an intergovernmental organization representing the customs administrations of 179 countries, which aims to enhance the effectiveness and efficiency of Customs administrations.

<sup>24</sup>AEOs include, for example, manufacturers, importers, exporters, brokers, ports, airports, terminal operators, warehouses, and distributors.

- 
- **Mutual recognition of AEO programs (AEO MRAs):** This occurs when Customs administrations agree to recognize one another's AEO programs and security features and to provide comparable benefits to members of the respective programs.

In the United States, C-TPAT is the designated AEO program and businesses participating in the program are AEOs. According to C-TPAT documentation, CBP has developed an AEO MRA process involving four phases: (1) a comparison of the program requirements to determine if the programs align on basic principles; (2) a pilot program of joint validation visits to determine if the programs align in basic practice; (3) the signing of an MRA; and (4) the development of mutual recognition operational procedures, primarily those associated with information sharing. MRAs are based on close working relationships between Customs administrations, which allow for the exchange of information, intelligence, and documents in an effort to assist countries in the prevention and investigation of Customs offenses.

The Coast Guard can also enter into MRAs that recognize international maritime security practices of other foreign governments. For example, the Coast Guard has a process in place to recognize the port inspection procedures of other countries.

**One Hundred Percent Scanning Requirement**

Although DHS's maritime security programs support the National Strategy for Global Supply Chain Security and the strategy's risk-informed security approach, the SAFE Port Act included requirements that pilot projects be established to test the feasibility of scanning 100 percent of U.S.-bound cargo containers at foreign ports.<sup>25</sup> Subsequently, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) required, among other things, that by July 2012, 100 percent of U.S.-bound cargo containers be scanned at foreign ports with both radiation

---

<sup>25</sup>6 U.S.C. § 981. This pilot was called the Secure Freight Initiative. A similar cargo-scanning requirement was enacted that same year by the Department of Homeland Security Appropriations Act, 2007 (Pub. L. No. 109-295, 120 Stat. 1355 (2006)) and is codified at 6 U.S.C. § 981a. Both statutes specify scanning as examination with both radiation detection equipment and nonintrusive imaging equipment. 6 U.S.C. §§ 981(a), 981a(a)(1).

---

detection and nonintrusive inspection (imaging) equipment before being placed onto U.S.-bound vessels.<sup>26</sup>

In June 2008 and in October 2009, we found that CBP faced numerous challenges in implementing the 100 percent scanning requirement at the pilot ports.<sup>27</sup> In October 2009, we recommended, among other things, that CBP conduct feasibility and cost-benefit analyses of implementing the 100 percent scanning requirement and provide the results to Congress along with any suggestions of cost-effective alternatives to implementing the 100 percent scanning requirement, as appropriate. CBP partially concurred with the recommendations but did not implement them. According to CBP officials, CBP does not plan to conduct these analyses related to achieving the 100 percent scanning requirement because the pilot project has been reduced in scope and currently there are no funds to conduct such analyses. In February 2012, we reported that the scanning challenges continued, and CBP achieved 100 percent scanning of U.S.-bound cargo containers at only one foreign pilot port where it was being attempted—Port Qasim, Pakistan.<sup>28</sup> In May 2012, the Secretary of Homeland Security announced a 2-year extension of the deadline—until July 2014—for implementing the requirement that cargo containers not enter the United States unless they are scanned at foreign ports prior to

---

<sup>26</sup>Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (amending 6 U.S.C. § 982(b)). Radiation detection equipment detects radiation being emitted from a container, and through a nonintrusive image scan, CBP can identify anomalies in a container's image that could, among other things, indicate the presence of dense material used to shield radioactive material.

<sup>27</sup>GAO, *Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers*, GAO-08-533T (Washington, D.C.: June 12, 2008), and *Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers*, GAO-10-12 (Washington, D.C.: Oct. 30, 2009).

<sup>28</sup>GAO, *Supply Chain Security: Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning*, GAO-12-422T (Washington, D.C.: Feb. 7, 2012).

being loaded on vessels.<sup>29</sup> In its report to Congress that same month, DHS stated that it recognizes the need to proceed with its container security programs in a manner that maximizes the security of maritime cargo and facilitates its movement. DHS added that it plans to continue working with other federal agencies and international partners to develop technology and enhance risk management processes, in addition to continuing its existing container security programs.<sup>30</sup> According to the January 2013 *National Strategy for Global Supply Chain Security Implementation Update*, DHS is working to identify potential alternatives to 100 percent scanning, and a senior DHS official told us that DHS's layered security strategy will be a key component of the alternative.<sup>31</sup>

### DHS Has Developed Models to Assess Foreign Port Risks, but CBP Has Not Assessed Whether Its CSI Locations Remain Valid

The Coast Guard and CBP, DHS components with maritime security responsibilities, have developed models to assess the risks of foreign ports and the cargo carried by vessels from these ports. The Coast Guard uses the model it developed to inform operational decisions for its IPS program and updates its assessment annually. In contrast, in 2009, CBP developed a risk model to begin the process of expanding its efforts to scan 100 percent of U.S.-bound container shipments, but the model was never implemented. As a result, it does not know whether the ports included in CSI remain valid.

<sup>29</sup>The 9/11 Act scanning provision includes possible extensions for containers loaded at a port or ports for which DHS certifies that at least two out of a list of specific conditions exist. Among others, these conditions include the following: (1) adequate scanning equipment is not available or cannot be integrated with existing systems, (2) a port does not have the physical characteristics to install the equipment, or (3) use of the equipment will significantly affect trade capacity and the flow of cargo. See 6 U.S.C. § 982(b)(4). The 9/11 Act also requires DHS to submit a report to Congress on whether it expects to seek to renew the extension 1 year after it takes effect. See id. § 982(b)(7). As of July 2013, DHS has not provided this report to Congress.

<sup>30</sup>DHS, *Scanning of Maritime Cargo Containers: Fiscal Year 2012 Report to Congress* (Washington, D.C.: May 3, 2012).

<sup>31</sup>The White House, *National Strategy for Global Supply Chain Security Implementation Update* (Washington, D.C.: January 2013).

---

**The Coast Guard Has  
Developed a Model to  
Regularly Assess Risks of  
Foreign Ports and Inform  
Operational Decisions**

The Coast Guard has developed a risk-informed model as part of its IPS program to regularly assess the potential threat foreign ports pose to the maritime supply chain and make operational decisions regarding foreign ports' security measures. According to the 2012 IPS program annual report, this risk model includes four components, summarized below, that help the Coast Guard focus IPS program resources.

**Country threat.** The Coast Guard uses security and commerce data as well as measures on government decision making, such as the prevalence of corruption, to assess the likelihood of terrorists using a foreign port to import WMDs or other contraband into the United States. In particular, the Coast Guard relies on CBP trade information, the U.S. Department of State's Security Environment Threat List, World Bank reports, and other data to determine whether countries represent a normal, medium, or high security risk.

**Foreign port assessment.** MTSA, as amended by the SAFE Port Act, requires the Coast Guard to reassess countries' ports every 3 years, and during these visits, IPS officials use two data checklists, one that assesses government performance and one that assesses facilities' performance.<sup>32</sup> The government performance checklist measures how well a government gathers and assesses information on security threats, and reviews and approves port facility security plans, among other things. The facilities performance checklist measures port security measures implemented to prevent unauthorized cargo and people from entering the port. Such security measures include, for example, perimeter security and access procedures for port facility employees and visitors.

**Country responsiveness.** The IPS model includes measures of the political, economic, and social conditions in a country to help determine whether countries are likely to efficiently utilize Coast Guard assistance. The model incorporates information on corruption, inflation, and "people measures," such as infant mortality rates and literacy rates.

**Country wealth.** The IPS model includes a measure of national income to determine if the country can afford to maintain security measures on its own or whether it is likely to require foreign assistance.

---

<sup>32</sup>46 U.S.C. § 70108(d).

---

According to the 2012 IPS program annual report, the Coast Guard combines these components into a single risk model and uses the results to make informed decisions on how to engage each country with the IPS program, including (1) how often to visit ports, (2) how many staff to assign to a particular visit, and (3) whether the country requires assistance. Specifically, the Coast Guard visits foreign ports in higher-risk countries more frequently (and with more IPS officials) than in ports in lower-risk countries, which we discuss later in this report. In addition, the IPS annual report states that the Coast Guard uses the country threat component of the IPS risk model to help determine which foreign vessels to board as part of its Port State Control program. The Coast Guard updates its risk model annually. While elements of the Coast Guard's risk model could be used to inform maritime container security efforts, there are limits regarding how it can be applied to maritime supply chain security because the IPS program is focused on assessing port security. Unlike the CBP risk model described below, the Coast Guard's model is not designed to assess the risk of maritime cargo shipments imported from foreign ports (e.g., transshipped cargo).

---

**CBP Considered Risk in Establishing Some CSI Ports, but Has Not Assessed Whether CSI Currently Covers the Riskiest Ports**

**CBP Selected Initial CSI Ports Largely on the Basis of Volume and Used More Risk Factors when Expanding CSI Locations**

In 2002, CBP selected the initial 23 CSI ports largely on the basis of the volume of U.S.-bound container cargo, but increased the number of risk factors in selecting additional ports as it expanded the CSI program beginning in 2003.<sup>33</sup> Specifically, according to CBP documentation, volume was a key criterion for assessing which foreign ports represented the greatest threat to the United States. Figure 4 shows the large number of containers shipped through the Port of Singapore, one of the original CSI ports.

---

<sup>33</sup>According to CBP officials, because of logistical factors such as the time necessary for negotiations with host governments and staffing CSI teams in foreign countries, initial CSI ports selected on the basis of volume sometimes did not begin operations until the expansion of CSI was under way.

**Figure 4: Partial View of the Port of Singapore**



Source: GAO.

After selecting these initial 23 ports, CBP subsequently added 35 ports to the CSI program from 2003 through 2007 on the basis of additional criteria, such as strategic threat factors and diplomatic or political considerations. Through these expansion efforts, in 2007 CBP reached its goal of staffing 58 CSI ports that, collectively, cover over 80 percent of U.S.-bound container shipments.<sup>34</sup> We reported in 2008 that CBP did not have plans to add other ports to the CSI program because, according to CBP, the costs associated with expanding the program would outweigh the potential benefits.<sup>35</sup>

<sup>34</sup>According to CBP officials, CBP entered into arrangements with New Zealand (April 2006) and Australia (November 2011) to remotely target U.S.-bound cargo container shipments from Auckland and Melbourne, respectively. Further, in August 2007, CBP began targeting containers at Shenzhen, China, that did not originally participate in CSI. According to CBP officials, CSI targeters in Shenzhen are also able to review and target shipments from Shekou, China, and can drive to that port to witness examinations. For the purposes of this report, we consider a port to be a CSI port if CBP has entered into an arrangement or otherwise coordinates with a foreign country to target U.S.-bound cargo container shipments from that port. Accordingly, we consider the number of CSI ports to be 61 rather than 58.

<sup>35</sup>GAO, *Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed*, GAO-08-187 (Washington, D.C.: Jan. 25, 2008).

---

CBP Developed a Risk Model for Expanding Container Security Efforts at High-Risk Ports, but It Was Never Implemented

In 2009, CBP developed a risk model in conjunction with DOE to begin the process of expanding its efforts to scan 100 percent of U.S.-bound container shipments for a related program, but the model was never implemented. In particular, in April 2009, the Secretary of Homeland Security approved the "strategic trade corridor strategy" as an approach to expanding CBP's efforts to scan U.S.-bound container cargo beyond the original pilot locations.<sup>36</sup> As part of this expansion effort, CBP developed a model—assisted by DOE—to rank potential foreign ports on the basis of risks associated with countries and maritime commerce, as well as the number and percentage of high-risk, U.S.-bound shipments processed. Specifically, DOE provided the country threat and shipping lane information from the model it used to identify and prioritize foreign ports for participation in the Megaports Initiative,<sup>37</sup> and CBP provided the high-risk shipment data from ATS. CBP and DOE completed their initial analyses in February 2009, which identified 356 potential expansion ports ranked by risk, and CBP narrowed the list down to 187 ports by considering only ports that had at least 1,000 shipments per year to the United States. CBP collaborated with DOE, the Department of State, and the intelligence community to prioritize 22 ports for expansion of 100 percent scanning efforts on the basis of such factors as the model's risk ranking and the volume of U.S.-bound cargo container shipments. CBP ultimately did not pursue this strategy, given cargo security program budget cuts and the Secretary of Homeland Security's decision to extend the deadline for 100 percent scanning until July 2014.

The results of the 2009 strategic trade corridor prioritization model show that the CSI program is operating at some of the riskiest foreign ports, but it also operates at ports that are less risky. Since the model focused on U.S.-bound maritime containerized cargo, its results could be used as a proxy measure to assess whether CSI ports coincide with those foreign locations that pose the greatest risk to the global supply chain. We

---

<sup>36</sup>The original pilot locations were Busan, South Korea; Puerto Cortes, Honduras; Qasim, Pakistan; Salalah, Oman; Southampton, United Kingdom; and Hong Kong.

<sup>37</sup>DOE established the Megaports Initiative in 2003 to deter, detect, and interdict nuclear or other radiological materials smuggled through foreign ports. The initiative funds the installation of radiation detection equipment at select ports overseas and trains host country personnel to use this equipment to scan cargo containers entering and leaving these ports—regardless of destination. The Megaports Initiative was intended to complement the CSI program. See GAO, *Combating Nuclear Smuggling: Megaports Initiative Faces Funding and Sustainability Challenge*, GAO-13-37 (Washington, D.C.: Oct. 31, 2012).

---

combined the risk rankings for the 356 ports in the 2009 model with fiscal year 2012 U.S.-bound shipment data and excluded ports with fewer than 1,000 U.S.-bound shipments per year, which narrowed the list to 138 ports.<sup>38</sup> Comparing the CSI ports with the results shows that CSI did not have a presence at about half of the ports CBP considered higher risk, and about one-fifth of the existing CSI ports were at lower-risk locations. Specifically, of the 61 current CSI ports, 57 had at least 1,000 U.S.-bound shipments in fiscal year 2012. Of these 57 CSI ports, 27 were within the top 50 riskiest ports, 18 ports were between the 51st and 100th riskiest ports, and 12 ports were not among the top 100 riskiest ports. Of the remaining 4 CSI ports, 3 had fewer than 1,000 U.S.-bound shipments and 1 port was not ranked in the 2009 risk model. According to CBP officials, CBP has not established CSI locations in 15 of the top 50 riskiest ports either because host governments have not been cooperative regarding CBP cargo examination requests or CBP was not able to negotiate an arrangement with host governments to establish CSI operations, as discussed below.

CBP officials stated that factors have changed since the model was developed in 2009, and they do not consider all of the same ports to be high risk at this time. For example, one potential expansion port the model classified as higher risk in 2009 now ships fewer containers to the United States, and CBP officials reported that they would not currently consider including this port in the CSI program. Further, according to CBP's fiscal year 2012 budget submission, CBP considered closing several CSI ports while maintaining CSI operations in strategically important ports. Given this information, and the fact that the number and location of CSI ports has generally not changed since 2009, the CSI program's current locations may not be in alignment with the highest-risk ports.

Because the CSI program depends on the willingness of sovereign host countries to participate in the program, there are challenges to implementing CSI and CBP efforts to negotiate with other countries to

---

<sup>38</sup>Fiscal year 2012 data were not available for 67 of the 356 ports in the 2009 model and were excluded from the analysis. However, only 3 of these ports were ranked among the top 100 riskiest ports. In addition, 3 CSI ports had fewer than 1,000 U.S.-bound shipments in fiscal year 2012 and were therefore not included in the analysis. We reached 138 ports with at least 1,000 U.S.-bound shipments instead of the 187 determined by CBP because we used fiscal year 2012 shipment data instead of the data included in the 2009 risk model.

---

expand the CSI program, and these efforts have not always been successful. CBP and the Department of State point to challenges in implementing CSI in high-risk countries, such as CBP officer safety, funding concerns, and the willingness of host country governments to facilitate requested cargo examinations of U.S.-bound shipments. CBP officials stated that CBP is not pursuing the strategic trade corridor strategy, but they noted that since the beginning of the CSI program, CBP has made efforts to negotiate to establish CSI ports within four countries that have ports representing potential significant risks. These efforts were not successful in three countries for political reasons. For example, the legislature in one of these countries did not approve the placement of CSI in its country. However, according to CBP officials, CBP has signed a declaration of principles to place CSI in an additional foreign country and estimates that CSI will be operational within this country by the end of fiscal year 2014.

**CBP Has Not Assessed the Risks of Foreign Ports that Ship Cargo to the United States since 2005**

CBP has not assessed the risk of foreign ports that ship cargo to the United States for its CSI program since completing the CSI expansion analysis in 2005. CBP officials stated they have not performed any such risk assessments since 2005 because CBP does not have any specific expansion plans for the CSI program. However, our work indicates that CBP may expand CSI. In particular, CBP's fiscal year 2013 and 2014 budget requests noted that CBP may expand CSI in the future to additional countries of strategic interest, if feasible; and CBP officials told us that CBP is finalizing negotiations with a foreign government to expand CSI to an additional port, as discussed above.

We acknowledge that CBP may face challenges in including foreign ports that ship the riskiest cargo to the United States in its CSI program, but expanding CSI without assessing the security risk posed by foreign ports is contrary to agency policy. In particular, according to the CSI Statement of Policy and Intent signed by the CBP Commissioner in April 2011, CBP is to prioritize CSI expansion locations in accordance with the *National Strategy for Global Supply Chain Security*, which states that the federal government should take a risk-informed approach to secure the global supply chain. Further, the SAFE Port Act provides that DHS/CBP is to assess the costs, benefits, and other factors associated with designation of a CSI port, including the level of risk for the potential compromise of containers by terrorists, or other threats as determined by DHS; the volume of cargo being imported to the United States directly from, or

---

being transhipped through, the foreign seaport; and the results of the Coast Guard's IPS assessments.<sup>39</sup>

In addition to not completing a risk assessment to help inform potential CSI expansion, CBP has also not assessed the risk of its current CSI ports—some of which have participated in CSI for more than a decade—to determine if they remain valid on the basis of risk. CBP officials stated that they have not conducted such an assessment because a couple of factors make it difficult to close CSI ports and reallocate resources to prospective new CSI ports. In particular, the officials stated that (1) removing CSI from a country might negatively affect political relations with the host government, and (2) uncertain CSI funding in future years could make it difficult for CBP to make plans to close lower-risk CSI ports and open new CSI ports at higher-risk locations. Specifically, CBP officials estimate that it could take about 1 year to close a CSI port and 2 years or more to open a new port, and, given budget uncertainties, CBP has not pursued such efforts.

It is unclear if the political and cost challenges CBP officials identified would affect any reallocation of CSI resources to prospective new CSI ports, but these challenges do not preclude CBP from assessing the risk of its current CSI locations. Regarding the impact of changes to the CSI program on political relations, CBP officials stated they routinely speak to host government officials during CSI evaluations about how to strengthen the program, but these officials said that the discussions have not specifically included the impact on relations with the host government of removing lower-risk ports from the CSI program. Further, it is unclear if reallocating resources from current CSI ports to higher-risk ports would ultimately increase costs because some costs—such as staffing costs and office space leases—could be lower in some of the new locations than costs in the lower-risk ports it would be leaving. Moreover, the DHS *National Infrastructure Protection Plan*<sup>40</sup> and our *Risk Management Framework*<sup>41</sup> state that risk assessments, the effectiveness of measures to deal with risks, and the costs of those measures are to inform decisions. Our framework also states that agencies should periodically

---

<sup>39</sup>U.S.C. § 945(b).

<sup>40</sup>DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009).

<sup>41</sup>See GAO-06-91.

---

evaluate the cost-effectiveness of their programs and that mechanisms for altering a program should be in place based on current risk data. In addition, the DHS *National Infrastructure Protection Plan* states that effective protective programs seek to use resources efficiently by focusing on actions that offer the greatest mitigation of risk for any given expenditure. The plan also states that risk management includes a feedback loop that continually incorporates new information, such as changing threats or the effect of actions taken to reduce or eliminate identified threats, vulnerabilities, or consequences.

We recognize that it may not be possible to include all the higher-risk ports in CSI because CSI requires the cooperation of sovereign foreign governments and because of concerns regarding the security of U.S. personnel that may be staffed in those countries. Nevertheless, given that CBP is no longer pursuing implementation of 100 percent scanning, it is important that CBP apply the risk management principles discussed above to CSI—a risk-informed program—to more effectively mitigate the threat of high-risk cargo before it is shipped to the United States. Periodically assessing the risk level of cargo shipped from foreign ports and using the results of these risk assessments to inform the CSI locations would help ensure that CBP is allocating its resources to provide the greatest possible coverage of high-risk cargo to best mitigate the risk of importing WMDs or other terrorist contraband into the United States through the maritime supply chain.

---

**DHS Has Taken Steps to Improve the Efficiency and Effectiveness of Its Maritime Container Security Programs, but Faces Constraints**

DHS, through the Coast Guard and CBP, has taken a number of steps to improve the efficiency and effectiveness of its maritime security programs to reduce global supply chain risks. In this regard, the Coast Guard's actions have primarily been focused on the IPS program. CBP has continued its efforts to expand or refine its C-TPAT and CSI programs, but faces host country political and legal constraints.

---

**The Coast Guard Has Worked to Reduce Global Supply Chain Risks by More Efficiently and Effectively Using IPS Resources**

The Coast Guard has worked to use resources more effectively and reduce risks at foreign ports and from U.S.-bound vessels through its IPS program by implementing a risk-informed model that prioritizes the countries to visit and provide with assistance. When the Coast Guard first implemented the IPS program in 2004, it was required by MTSA to assess the effectiveness of antiterrorism measures maintained in ports where U.S. vessels call or from which vessels depart for the United States. As a result, the Coast Guard focused on completing initial visits of foreign ports to determine ISPS Code compliance, but did not have a methodology to prioritize follow-up visits and help countries increase their level of port security. To accomplish these goals, in 2005, the Coast Guard began developing its IPS risk model to assess the risks of foreign ports and prioritize assistance, which it fully integrated into IPS operations in 2011. The Coast Guard classifies countries as normal, medium, or high security risks and completes port security checklists during foreign port visits.

**The Coast Guard Uses Its Risk Assessments to Manage Port Visits and Allocate Foreign Assistance**

According to the 2012 IPS program annual report, the Coast Guard uses the results of its risk assessments to help determine the amount of resources needed to visit foreign countries' ports, board foreign vessels, and track port security improvements. Specifically, the Coast Guard uses the risk model results to more efficiently and effectively allocate resources to help ensure that visits to foreign ports in higher-risk countries occur more frequently (and with more IPS officials) than to ports in lower-risk countries.<sup>42</sup> Table 1 provides information on Coast Guard IPS program visits, by country risk level, for fiscal year 2012.

---

<sup>42</sup>Coast Guard officials visit foreign ports to evaluate their antiterrorism security measures against established ISPS Code standards.

**Table 1: Coast Guard International Port Security Program Visits, by Country Risk Level, for Fiscal Year 2012**

Foreign country risk level	Number of foreign countries visited <sup>a</sup>	Average number of staff days per visit <sup>b</sup>	Average cost per visit <sup>c</sup>
Normal risk	13	14	\$9,926
Medium risk	18	29	\$27,193
High risk	23	37	\$38,214

Source: GAO analysis of Coast Guard data.

<sup>a</sup>Through the International Port Security program, the Coast Guard makes a determination of country, not port, risk level.

<sup>b</sup>Staff days are cumulative for all Coast Guard staff involved in foreign port visits. According to Coast Guard officials, many visits were the result of multiple trips and often included different staff on the team.

<sup>c</sup>According to Coast Guard officials, costs reflect travel and per diem costs as well as any funds provided to the U.S. embassy for translators, additional security, and in-country flights, among other things. They do not reflect any salary or overhead costs.

IPS program officials we met with that are responsible for assessing ports in Africa and Southeast Asia stated that this risk-informed approach helps the Coast Guard more efficiently use its resources. Further, the IPS program has enabled the Coast Guard to measure foreign countries' port security based on improvements its officials observe when completing foreign port visits. According to the 2012 IPS program annual report, port assessment scores have improved worldwide since the Coast Guard initiated the IPS program in 2004. The Coast Guard attributes this success, in part, to implementation of the IPS risk model.

According to the 2012 IPS program annual report, the Coast Guard also uses the results of the IPS model to allocate foreign assistance. The risk model includes (1) country threat information; (2) port visit results; (3) a determination of which countries are most likely to benefit from assistance to improve port security, such as port security training; and (4) the individual country's ability to best use assistance funds and sustain security efforts, as discussed earlier in this report. The 2012 report also states that Coast Guard officials are to use this information to direct resources to those foreign countries where they believe the return on investment will be greatest. Further, this report states that the Coast Guard uses the results of the IPS risk model to help determine which foreign vessels to board as part of its Port State Control program. The risk-based screening tool the Coast Guard uses to select vessels to board assigns point values to various risk factors, such as country threat data

---

MRAs May Allow the Coast Guard to Allocate Resources More Efficiently

from the IPS risk model. In addition, the Coast Guard boards foreign vessels that have recently stopped in higher-risk ports (i.e., countries that have not substantially implemented the ISPS Code).

In addition to prioritizing resources through its IPS risk model, the Coast Guard has worked with foreign governments to mutually recognize each other's maritime security programs, which can more efficiently use IPS resources and reduce risks. For example, in September 2012, the Coast Guard signed a memorandum of understanding (MOU) with the European Union that establishes a process for mutually recognizing security inspections of each other's ports.<sup>43</sup> The European Union has developed regulations for the consistent implementation of the ISPS Code by its member states and established a process for verifying the effectiveness of its member states' maritime security measures. This process includes European Union inspections of member states' ports that result in reports that (1) identify any nonconformities with the regulations and (2) make recommendations to address any nonconformities.

Under the MOU procedures, the Coast Guard recognizes a successful European Union inspection of its member states' ports in the same manner as it would recognize a successful country visit by Coast Guard IPS inspectors. Coast Guard IPS officials stated that they have collaborated with their European counterparts to develop standard operating procedures for these port inspections and they were used in a recent joint inspection of a container facility in Felixstowe, the United Kingdom. According to DHS documents and Coast Guard IPS officials in Europe, by signing this MOU, the Coast Guard plans to reassign some IPS officials from Europe to Africa, where certain countries are having more difficulties in implementing effective antiterrorism measures in their ports. Coast Guard IPS officials reported, however, that a trade-off of signing the MOU is that its IPS officials will not have the same opportunities to have face-to-face interactions and share port security information and practices directly with their European Union counterparts as in the past. Despite this trade-off, the Coast Guard IPS officials stated that entering into such arrangements increases efficiencies and noted that they intend to negotiate additional MOUs with other foreign governments that have strong port inspection programs.

---

<sup>43</sup>According to DHS officials, the European Union characterizes its port visits as "inspections."

---

**CBP Has Worked to More Efficiently Use Resources and Expand Its C-TPAT Membership****CBP Has Taken Steps to More Efficiently Use Resources by Negotiating MRAs**

CBP has worked with foreign partners to mutually recognize each other's AEO programs to more efficiently use resources while continuing to reduce risks to the global supply chain. According to the World Customs Organization, as of June 2013, there were 25 AEO programs worldwide, other than C-TPAT, with which CBP could enter into an MRA. As part of the evaluation of a foreign partner's capacity for entering into an MRA, CBP conducts joint validations with the other partner to ensure that a partner's AEO program has security standards that are equivalent to those required by the C-TPAT program. CBP officials stated that CBP does not pursue mutual recognition with a Customs administration that does not have an equivalent AEO program in place because doing so could compromise the security of U.S.-bound container shipments. As of July 2013, CBP had signed MRAs with seven foreign Customs administrations—New Zealand in 2007, Canada and Jordan in 2008, Japan in 2009, the Republic of (South) Korea in 2010, and the European Union and the Taipei Economic and Cultural Representative Office (Taiwan) in 2012—and is in the process of negotiating MRAs with five other partners. CBP officials stated that they expect to complete MRA negotiations with one partner by the end of fiscal year 2013 and that they generally complete one or two MRAs each year.

To help foreign countries establish AEO programs, CBP officials stated that the C-TPAT program provides training and technical assistance for foreign Customs agencies that request technical assistance. As of April 2013, CBP officials reported that C-TPAT has provided assistance to about 70 foreign countries and noted that this assistance improves global supply chain security. Further, CBP officials told us that the goal of this assistance is to establish AEO-MRAs with foreign Customs agencies as a means to increase efficiencies in supply chain security efforts. According to CBP officials, by relying on MRA partners to validate supply chain security procedures overseas, CBP is able to operate more efficiently by reducing the costs associated with conducting security validations. For example, in 2010, CBP completed a study on AEO validation visits conducted on its behalf in Japan and Canada by the respective host governments. On the basis of cost data from prior validation visits, CBP estimates the C-TPAT program saved over \$290,000 and over 1,500 staff hours by accepting the 90 validations completed by the Japanese and

---

Canadian governments during 2009 and 2010.<sup>44</sup> Further, according to CBP officials, mutual recognition leads to a common understanding of global supply chain security standards, resulting in greater program efficiency and a streamlined validation process by reducing the number of redundant validations. As a result, mutual recognition enables CBP to focus its resources on higher-risk supply chains. CBP officials also stated that AEO program officials are in a better position to conduct validations of companies within their respective AEO programs because these officials are proficient in the local language and are more familiar with the companies' supply chains.

MRAs can increase efficiencies in the C-TPAT program, but CBP faces challenges in implementing MRAs. According to C-TPAT data, since 2009, CBP has accepted over 480 validations conducted by staff from foreign governments that have signed MRAs with the United States. Further, these data show that the number of validations conducted by MRA partners has increased significantly each year from 2009 (26) through 2012 (285), and CBP officials stated that they expect the number of validations to continue to increase because the European Union and Taiwan—two of the United States' largest trading partners—are expected to conduct more validations in 2013. While MRAs have resulted in increased efficiencies, CBP and foreign government officials we met with identified challenges in implementing MRAs. For example, CBP and foreign government officials we met with stated that exchanging data across information technology systems can be difficult, and government officials from one foreign partner stated that differences in privacy laws between partners can create additional hurdles to information sharing. As a result, it may take time for the benefits to be evident to the AEO partners. Specifically, private sector trade officials in one country we visited reported that they had not yet realized the benefits of the MRA through reduced inspections of their shipments at U.S. ports. In addition, World Customs Organization officials we met with said that it may be difficult to document the benefits of MRAs through reduced inspections because U.S. agencies other than CBP also have their own inspection procedures for imported cargo that are not part of any MRA. For example, according to CBP, the Food and Drug Administration has its own inspection process. As a result, MRA participants' shipments could still be

---

<sup>44</sup>The study did not account for any costs associated with negotiating the MRAs. C-TPAT has not conducted any cost studies related to the MRAs with Jordan, New Zealand, Taiwan, South Korea, or the European Union.

---

slowed. According to CBP officials, CBP is working with other federal agencies to harmonize the inspection process at ports of entry and accelerate inspection decision making to address this issue.

CBP has entered into AEO-MRAs with other partners, but does not have plans to negotiate Customs-to-Customs MRAs. Under a Customs-to-Customs MRA, joint activities, such as identifying cargo for examination, would not require the placement of CBP targeters in foreign ports under programs like CSI. CBP officials said they do not have plans to negotiate Customs-to-Customs MRAs because they are much more difficult to achieve than AEO-MRAs, in part, because of the difficulties in ensuring Customs practices are applied consistently. For example, CBP officials said that Customs-to-Customs MRAs would need to include a broader validation of foreign Customs administrations' practices. World Customs Organization officials we met with concurred that achieving mutual recognition of Customs controls is difficult and noted that the focus of Customs administrations worldwide is on negotiating AEO-MRAs rather than Customs-to-Customs MRAs.

**CBP Has Made Efforts to Improve Efficiency and Effectiveness by Increasing C-TPAT Membership**

CBP has also made efforts to improve the efficiency and effectiveness of its C-TPAT program—and thus the security of the global supply chain—by increasing the number and category of C-TPAT members. For example, CBP has increased C-TPAT membership by conducting outreach events to increase awareness of the C-TPAT program and incentives. From fiscal years 2008 through 2012, the number of C-TPAT members increased by 15 percent—from 8,882 to 10,425. According to the 2013 DHS Annual Performance Report, as of fiscal year 2012, C-TPAT members account for more than 50 percent of all U.S. cargo imports (by value), which exceeds CBP's performance target goal of 45 percent. Further, as part of C-TPAT's membership expansion efforts, the program is considering adding two supply chain sectors—exporters and distribution centers.<sup>45</sup> CBP officials reported that C-TPAT selected these sectors because they can have a direct impact in securing the global supply chain. Moreover, according to the 2012 C-TPAT Strategy Action Plan, increased membership in the C-TPAT program could allow U.S. ports of entry to operate more efficiently because CBP officials at these

---

<sup>45</sup>As of July 2013, C-TPAT membership is spread over 10 different supply chain sectors, such as importers and port operators.

---

Staffing Challenges and  
Members' Compliance with  
Security Requirements Limit  
CBP Efforts to Improve C-  
TPAT Effectiveness

ports would be able to focus CBP's targeting and inspection resources on a smaller percentage of high-risk shipments.

Although expansion of C-TPAT membership should increase program efficiencies systemwide, CBP faces challenges in increasing C-TPAT effectiveness because of staffing challenges. In particular, while the C-TPAT program has continued to expand in size and scope in recent years, staffing within the program has decreased. Specifically, according to CBP officials, as of July 2013, the C-TPAT program had 155 staff, down from a peak of 196 staff in January 2011. CBP plans to take several steps to address this staffing challenge. For example, CBP officials reported that as of July 2013, C-TPAT is working with CBP's Office of Human Resources to hire 11 additional Supply Chain Security Specialists.<sup>46</sup> Furthermore, according to fiscal year 2014 CBP budget documentation, CBP plans to extend the C-TPAT revalidation cycle to once every 4 years as mandated by the SAFE Port Act rather than accelerating the revalidation schedule to once every 3 years as CBP had previously done. Moreover, C-TPAT officials reported that CBP anticipates a reduction in foreign validation visits by its specialists through the implementation of MRAs.

An additional challenge to C-TPAT program effectiveness is that C-TPAT partners' compliance rates with program security requirements decreased from almost 100 percent in fiscal year 2008 to about 95 percent in fiscal year 2012. According to CBP documentation, the overall compliance rate decreased after CBP strengthened C-TPAT security criteria and increased program oversight. CBP reported that C-TPAT is working with C-TPAT partners to explain the enhanced security criteria to ensure they understand the validation requirements. CBP officials said that they expect this will lead to improvements in C-TPAT partners' compliance with the security requirements.

---

<sup>46</sup>Supply Chain Security Specialists are responsible for responding to the needs of C-TPAT partners, as well as conducting training and outreach efforts with local law enforcement, CBP components, and other entities.

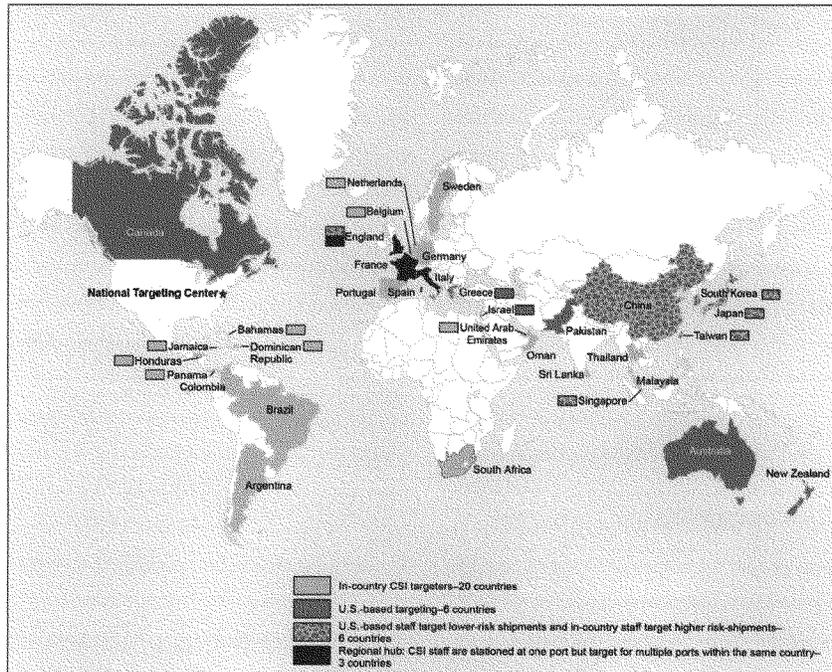
---

**CBP Revised CSI in  
Response to Budget Cuts,  
but Efficiencies and  
Effectiveness Are Limited  
by Political and Legal  
Factors**

**CBP Revised CSI Targeting  
Approaches to Address Budget  
Cuts**

As a result of reduced program budgets in recent years, CBP has implemented CSI changes to take advantage of improvements in technology and more efficiently use its CSI targeters, but efficiencies are limited by host country political and legal factors. Specifically, CSI program expenditures declined by more than \$50 million from fiscal years 2008 through 2012, and this cut led to changes in how CBP has staffed its CSI ports. As shown in figure 5, CBP employs a variety of approaches in targeting and examining U.S.-bound containerized cargo imported from CSI countries. These targeting approaches are explained below.

**Figure 5: Map Showing the Variety of Targeting Approaches Customs and Border Protection Uses in Container Security Initiative Countries as of July 2013**



Source: GAO; Map Resources (map)

Notes: Targeting refers to the review of shipment data and additional information by CBP officials to identify high-risk shipments with a potential nexus to terrorism.

CSI ports in England utilize both the regional hub and a mixture of in-country and U.S.-based targeting approaches.

CBP coordinates targeting of U.S.-bound cargo container shipments in 34 countries that covers 61 foreign ports.

---

**National Targeting Center-Cargo (NTC-C) support.** In April 2005, we recommended that CBP revise the CSI targeting approach to consider what functions need to be performed at CSI ports and what functions can be performed in the United States.<sup>47</sup> CBP agreed with this recommendation and, in January 2009, began transferring some CSI staff from overseas ports to perform targeting remotely from the NTC-C. According to CBP officials, NTC-C staff are less costly than overseas staff.<sup>48</sup> Under this revised targeting approach, NTC-C targeters review U.S.-bound shipments from foreign ports in 6 CSI countries. For those shipments that NTC-C targeters determine to be high risk or suspect, NTC-C targeters request that host government Customs officials complete examinations and electronically provide the results to NTC-C staff. Further, according to CSI officials, NTC-C targets all shipments ATS categorizes as lower risk in an additional 6 CSI countries so that CSI targeters in those 6 countries can concentrate their reviews on the higher-risk shipments. According to CBP officials, implementation of this targeting approach allows CBP to staff high-volume ports with fewer CSI targeters. Our analysis of CSI staffing data shows that staffing of CBP targeters that support CSI at the NTC-C increased by 56 percent from fiscal years 2009 through 2012—from 27 to 42. Changes in CBP's staffing of in-country targeters are discussed below.

**Regional hub model.** In 2011 and 2012, CBP implemented a regional hub model whereby CSI targeters are stationed at one port but target for multiple ports within the same country to reduce staff and thereby increase efficiencies. Under this targeting approach, host government Customs officials at remote ports complete the container examinations and electronically provide the results to CSI targeters at the regional hub. According to CBP host government officials, implementation of the regional hub is possible because of improvements in technology that allow for better and more timely transmission of image scans. Of the 13 countries with multiple CSI ports, 3 employ the regional hub model—England, France, and Italy. CBP officials reported that since implementing

---

<sup>47</sup>GAO, *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts*, GAO-05-557 (Washington, D.C.: Apr. 26, 2005).

<sup>48</sup>NTC-C analyzes advance cargo information using ATS prior to U.S.-bound cargo being loaded on to vessels in foreign ports. NTC-C also promotes information sharing with other federal agencies and foreign governments to detect and address threats at U.S. and foreign ports.

---

the regional hub model, CBP has reduced the number of CSI targeters in these 3 countries by 45 percent—from 20 in October 2011 to 11 as of April 2013. According to both CBP targeters stationed in England and their British counterparts, implementation of the regional hub model has not affected the quality or number of scans of U.S.-bound container shipments.

Although implementation of the regional hub model increases efficiencies, CBP officials stated that they do not have plans to implement the regional hub model in other countries in the near future because of host country political and legal reasons. For example, CBP officials told us that CBP considered implementing the regional hub model in one country; however, the host government preferred to maintain the face-to-face interaction between the CSI targeters and their host government counterparts at each CSI port as a means to improve information exchanges and increase collaboration. Further, according to CBP and government officials in one country, a national law precludes the transmission of electronic scanned images other than to host government Customs officials. As a result, CSI targeters must be present at each CSI port in order to view the scanned container images.

**In-country CSI targeters.** Where possible, CBP has shifted from the initial CSI targeting approach that was heavily dependent on the placement of targeters at foreign ports to an approach that takes advantage of improvements in technologies for transmitting image scans, as addressed earlier. Specifically, from fiscal years 2009 through 2012, CBP reduced the number of CSI targeters stationed at foreign ports by 50 percent—from 153 to 77. However, as noted above, CBP increased the number of CSI targeters stationed at the NTC-C during the same time period. CBP maintains in-country targeters in 20 of the 34 CSI countries. A key benefit of maintaining CSI targeters at these ports is the relationship built with host government counterparts. CSI targeters in all 6 foreign countries we visited and host government officials in 5 of the 6 countries we visited told us that personal relationships and trust that are established between CSI targeters and host country government officials from having the CSI targeters in country are fundamental to the success of the CSI program.<sup>49</sup> In particular, the CSI targeters and host government

---

<sup>49</sup>Officials in one foreign country we visited stated that in-country CBP targeters were not important for successful CSI operations.

---

officials in these 5 countries agree that the physical presence of CSI staff increases information sharing and improves collaboration. Further, host country Customs officials in 3 of the 6 countries we visited stated that the presence of CSI targeters contributed to the development or enhancement of their countries' cargo targeting programs.

According to our review of CBP performance data, changes in staffing levels in recent years have not negatively affected the effectiveness of the CSI program. In particular, CBP tracks two performance measures—(1) the percentage of U.S.-bound cargo container shipments that are reviewed by CSI targeters and (2) the percentage of U.S.-requested cargo examinations that are completed by host countries. According to CBP data from fiscal years 2009 through 2012, CSI targeters met their target goal of reviewing 100 percent of the U.S.-bound cargo shipments. Moreover, the percentage of U.S.-requested examinations of U.S.-bound cargo shipments completed by host countries increased from 93 percent in fiscal year 2009 to 98 percent in fiscal year 2012, although CBP did not meet the target goal of 100 percent. CBP reported that CSI relies on the voluntary cooperation of host nation Customs officials and that CBP works with the host ports to resolve examination issues as they arise in an effort to increase the percentage of U.S.-bound shipments that are examined.

**CBP Has Made Efforts to Expand the Scope of CSI beyond WMD to Improve Effectiveness**

CBP has made efforts to expand the scope of CSI targeting beyond WMD, where possible, in an effort to increase the effectiveness of the CSI program. While the priority focus of CSI is to prevent WMD and other terrorist contraband from entering the United States through cargo containers, the April 2011 CSI Statement of Policy and Intent prioritized expanding the scope of CSI beyond WMD, among other things. In particular, according to the CSI Strategy Action Plan, as well as CSI program officials with whom we met, CBP is negotiating with government officials in foreign countries where CBP has CSI targeters to expand the focus of CSI's targeting efforts beyond WMD to include other contraband, such as illicit drugs, illegal weapons, and counterfeit goods (intellectual property right violations). The CBP officials we met with noted, however, that expanding the scope of CSI targeting efforts beyond WMD is ultimately at the discretion of the host governments with whom CBP has negotiated guidelines for CSI program operations. While two of the six CSI countries that we visited allow CSI staff to target U.S.-bound cargo container shipments for contraband other than WMD, the remaining four countries generally limit targeting and examinations to cargo containers suspected of containing WMD. Government officials from one of these four countries stated it is CBP's responsibility to scan containers for other

---

suspected contraband, such as illicit drugs, once the containers arrive in the United States. Customs officials from another one of these four countries stated they do not have the resources to devote to scanning U.S.-bound containers that may be at risk for containing contraband other than WMD. According to CBP officials, though, expanding the scope of targeting at foreign ports by its CSI targeters has not resulted in additional costs to CBP in terms of numbers of targeters or funding.

---

## Conclusions

Reducing risks to the global maritime supply chain is critical because foreign ports and the cargo carried by vessels from these ports are vital to the U.S. economy. DHS has made progress in reducing some maritime supply chain risks through its various maritime container security programs. The Coast Guard has developed a port security risk model that it annually updates and uses to assess port facility security, inform operational decisions, and direct resources. In contrast, CBP has not assessed the risks of foreign ports that ship cargo to the United States to determine whether its existing CSI locations remain valid since 2005. Although there have been no known incidents of cargo containers being used to transport WMD, the maritime supply chain remains vulnerable to attacks. We recognize that it may not be possible to include all of the higher-risk ports in CSI because CSI requires the cooperation of sovereign foreign governments. However, DHS and GAO risk management practices state that agencies should periodically evaluate the effectiveness of their programs and that mechanisms should be in place for altering a program based on current risk data. Periodically assessing the risk level of cargo shipped from foreign ports and using the results of these risk assessments to inform any future expansion of CSI to additional locations as well as determining whether changes need to be made to existing CSI ports would help ensure that CBP is allocating its resources to provide the greatest possible coverage of high-risk cargo to best mitigate the risk of importing WMD or other terrorist contraband into the United States through the maritime supply chain.

---

## Recommendations for Executive Action

To better ensure the effectiveness of the CSI program, we recommend that the Secretary of Homeland Security direct the Commissioner of U.S. Customs and Border Protection to periodically assess the supply chain security risks from all foreign ports that ship cargo to the United States and use the results of these risk assessments to (1) inform any future expansion of CSI to additional locations and (2) determine whether changes need to be made to existing CSI ports and make adjustments as appropriate and feasible.

---

### Agency Comments and Our Evaluation

In August 2013, we requested comments on a draft of this report from the Departments of Homeland Security and State. Both departments provided technical comments, which we have incorporated into the report, as appropriate. In addition to its technical comments, DHS provided an official letter for inclusion in the report, which can be seen in appendix II. In its letter, DHS stated it concurred with the recommendation and plans to develop a process for conducting periodic assessments of the supply chain security risks from all ports that ship cargo to the United States and use information from the assessments to determine if future expansion or adjustments to CSI locations are appropriate.

---

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Secretaries of State and Homeland Security, appropriate congressional committees, and other interested parties. This report will also be available at no charge on GAO's website at <http://www.gao.gov>.

If you or your staff have any questions, please contact me at (202) 512-9610 or [caldwells@gao.gov](mailto:caldwells@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Staff acknowledgments are provided in appendix III.



Stephen L. Caldwell  
Director  
Homeland Security and Justice

## Appendix I: Information on Foreign Ports That Coordinate Maritime Cargo Container Security Efforts with U.S. Customs and Border Protection

This appendix provides information on the foreign ports that either participate directly in the Container Security Initiative (CSI) program or that U.S. Customs and Border Protection (CBP) otherwise coordinates with to review and secure U.S.-bound cargo container shipments. As of July 2013, CBP was coordinating targeting of U.S.-bound cargo container shipments with 61 foreign ports. Table 2 lists these ports according to the date the ports began conducting operations with CBP and also provides information on, among other things, the volume of U.S.-bound shipments passing through the seaport in fiscal year 2012 and the targeting approach employed.

**Table 2: Foreign Ports That CBP Coordinates with Regarding Maritime Container Shipment Examinations, as of July 2013 (Listed by Date Port Began CSI Operations)**

Seaport	Country	Date port began CSI operations	Number of U.S.-bound maritime container shipments (fiscal year 2012)	Targeting approach
1 Vancouver	Canada	2/20/2002	75,226	Remote <sup>a</sup>
2 Halifax	Canada	3/25/2002	11,731	Remote
3 Montreal	Canada	3/25/2002	257	Remote
4 Rotterdam	Netherlands	9/2/2002	177,448	In-country <sup>b</sup>
5 Le Havre	France	12/2/2002	130,577	Regional hub <sup>c</sup>
6 Bremerhaven	Germany	2/2/2003	379,662	In-country
7 Hamburg	Germany	2/9/2003	184,163	In-country
8 Antwerp	Belgium	2/23/2003	268,479	In-country
9 Singapore	Singapore	3/10/2003	428,730	NTC-C support <sup>d</sup>
10 Yokohama	Japan	3/24/2003	42,953	In-country
11 Hong Kong	China	5/5/2003	938,821	NTC-C support
12 Gothenburg	Sweden	5/23/2003	14,007	In-country
13 Felixstowe	United Kingdom	5/24/2003	54,926	Regional hub/NTC-C support
14 Genoa	Italy	6/16/2003	151,464	Regional hub
15 La Spezia	Italy	6/23/2003	139,382	Regional hub
16 Busan	South Korea	8/4/2003	867,627	NTC-C support
17 Durban	South Africa	12/1/2003	11,807	In-country
18 Port Kelang	Malaysia	3/8/2004	7,393	In-country
19 Tokyo	Japan	5/21/2004	139,659	NTC-C support
20 Piraeus	Greece	7/27/2004	9,746	Remote
21 Algeiras	Spain	7/30/2004	33,733	In-country
22 Kobe	Japan	8/6/2004	77,790	In-country

**Appendix I: Information on Foreign Ports That Coordinate Maritime Cargo Container Security Efforts with U.S. Customs and Border Protection**

Seaport	Country	Date port began CSI operations	Number of U.S.-bound maritime container shipments (fiscal year 2012)	Targeting approach
23 Nagoya	Japan	8/6/2004	74,402	In-country
24 Laem Chabang	Thailand	8/13/2004	95,551	In-country
25 Tanjung Pelepas	Malaysia	8/16/2004	84,337	In-country
26 Naples	Italy	9/30/2004	19,024	Regional hub
27 Liverpool	United Kingdom	10/19/2004	35,273	Regional hub/NTC-C support
28 Thamesport	United Kingdom	10/19/2004	27,818	Regional hub/NTC support
29 Southampton	United Kingdom	10/19/2004	50,357	Regional hub/NTC-C support
30 Tilbury	United Kingdom	10/19/2004	2,382	Regional hub/NTC-C support
31 Gioai Tauro	Italy	10/29/2004	12,381	Regional hub
32 Zeebrugge	Belgium	10/29/2004	25	In-country <sup>3</sup>
33 Livorno	Italy	12/16/2004	77,299	Regional hub
34 Marseilles	France	1/7/2005	16,378	Regional hub
35 Dubai	United Arab Emirates	3/26/2005	13,350	In-country
36 Shanghai	China	4/12/2005	1,900,294	NTC-C support
37 Shenzhen	China	6/24/2005	1,475,210	NTC-C support
38 Kaohsiung	Taiwan	7/25/2005	630,732	NTC-C support
39 Santos	Brazil	9/21/2005	50,816	In-country
40 Colombo	Sri Lanka	9/29/2005	127,432	In-country
41 Buenos Aires	Argentina	11/17/2005	20,791	In-country
42 Lisbon	Portugal	12/14/2005	36,903	In-country
43 Port Salalah	Oman	3/8/2006	97,450	In-country
44 Puerto Cortes	Honduras	3/25/2006	67,996	In-country
45 Auckland <sup>d</sup>	New Zealand	4/1/2006	47,244	Remote
46 Chi-lung	Taiwan	9/25/2006	97,476	In-country
47 Valencia	Spain	9/25/2006	106,118	In-country
48 Caucedo	Dominican Republic	9/26/2006	24,843	In-country
49 Barcelona	Spain	9/27/2006	41,763	In-country
50 Kingston	Jamaica	9/28/2006	75,607	In-country
51 Freeport	Bahamas	9/29/2006	66,912	In-country
52 Qasim	Pakistan	4/30/2007	46,486	Remote
53 Shekou	China <sup>a</sup>	08/01/2007	60,019	NTC-C support
54 Chiwan	China	8/1/2007	138,069	NTC-C support
55 Balboa	Panama	8/27/2007	76,380	In-country

**Appendix I: Information on Foreign Ports That Coordinate Maritime Cargo Container Security Efforts with U.S. Customs and Border Protection**

Seaport	Country	Date port began CSI operations	Number of U.S.-bound maritime container shipments (fiscal year 2012)	Targeting approach	
56	Cartagena	Colombia	9/13/2007	52,682	In-country
57	Ashdod	Israel	9/17/2007	543	Remote
58	Haifa	Israel	9/25/2007	36,490	Remote
59	Colon	Panama	9/28/2007	50,481	In-country
60	Manzanillo	Panama	9/28/2007	77,030	In-country
61	Melbourne <sup>1</sup>	Australia	11/1/2011	37,730	Remote

Source: GAO presentation of CBP data.

<sup>1</sup>The remote targeting approach relies on host government Customs officials to complete the container examinations and electronically provide the results of any container image scans to U.S.-based CBP targeters.

<sup>2</sup>The in-country targeting approach places CBP targeters at CSI ports, who directly coordinate with host government Customs officials to examine containers and obtain the results of the examinations.

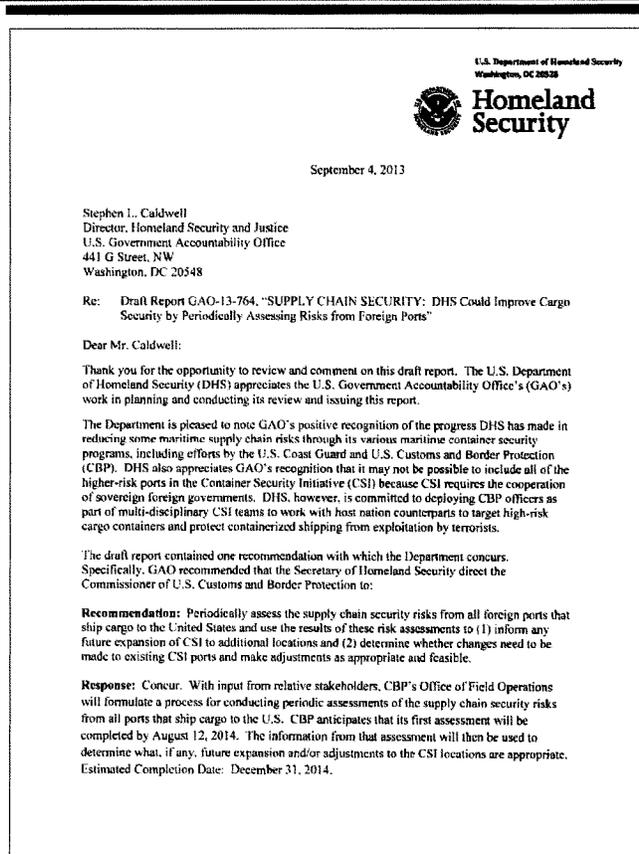
<sup>3</sup>Under the regional hub targeting approach, CSI staff are stationed at one port but target for multiple ports within the same country to increase efficiencies. Host government Customs officials at remote ports complete the container examinations and electronically provide the results to CSI targeters at the regional hub.

<sup>4</sup>The National Targeting Center-Cargo (NTC-C) targeting approach relies on in-country CBP targeters to review higher-risk shipments and U.S.-based CBP targeters to review lower-risk shipments. NTC-C analyzes advance cargo information before shipments reach the United States.

<sup>5</sup>According to CBP officials, CSI targeters in Antwerp also target U.S.-bound container shipments exported from Zeebrugge and drive to that port to participate in examinations, as necessary.

<sup>6</sup>According to CBP officials, CBP entered into arrangements with New Zealand and Australia to remotely target U.S.-bound cargo container shipments from Auckland and Melbourne, respectively. Further, in August 2007, CBP began targeting containers at Shenzhen, China, that did not originally participate in CSI. According to CBP officials, CSI targeters in Shenzhen are also able to review and target shipments from Shekou, China, and can drive to that port to witness examinations. For the purposes of this report, we consider a port to be a CSI port if CBP has entered into an arrangement or otherwise coordinates with a foreign country to target U.S.-bound cargo container shipments from that port. Accordingly, we consider the number of CSI ports to be 61 rather than 58.

## Appendix II: Comments from the Department of Homeland Security



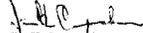
---

**Appendix II: Comments from the Department  
of Homeland Security**

---

Again, thank you for the opportunity to review and provide comments on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,



Jim H. Crumpacker  
Director  
Departmental GAO-OIG Liaison Office

---

## Appendix III: GAO Contact and Staff Acknowledgments

---

### GAO Contact

Stephen L. Caldwell, Director (202) 512-9610 or [caldwells@gao.gov](mailto:caldwells@gao.gov)

---

### Staff Acknowledgments

In addition to the contact named above, Christopher Conrad (Assistant Director), Josh Diosomito, and Paul Hobart made key contributions to this report. Also contributing to this report were Charles Bausell, Frances Cook, Stanley Kostyla, and Lara Miklozek.

---

## Related GAO Products

---

*Combating Nuclear Smuggling: Megaports Initiative Faces Funding and Sustainability Challenges.* GAO-13-37. Washington, D.C.: October 31, 2012.

*Supply Chain Security: CBP Needs to Conduct Regular Assessments of Its Cargo Targeting System.* GAO-13-9. Washington, D.C.: October 25, 2012.

*Maritime Security: Progress and Challenges 10 Years after the Maritime Transportation Security Act.* GAO-12-1009T. Washington, D.C.: September 11, 2012.

*Supply Chain Security: Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning.* GAO-12-422T. Washington, D.C.: February 7, 2012.

*Homeland Security: DHS Could Strengthen Acquisitions and Development of New Technologies.* GAO-11-829T. Washington, D.C.: July 15, 2011.

*Maritime Security: Responses to Questions for the Record.* GAO-11-140R. Washington, D.C.: October 22, 2010.

*Supply Chain Security: DHS Should Test and Evaluate Container Security Technologies Consistent with All Identified Operational Scenarios to Ensure the Technologies Will Function as Intended.* GAO-10-887. Washington, D.C.: September 29, 2010.

*Supply Chain Security: CBP Has Made Progress in Assisting the Trade Industry in Implementing the New Importer Security Filing Requirements, but Some Challenges Remain.* GAO-10-841. Washington, D.C.: September 10, 2010.

*Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers.* GAO-10-12. Washington, D.C.: October 30, 2009.

*Supply Chain Security: CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain.* GAO-08-538. Washington, D.C.: August 15, 2008.

---

**Related GAO Products**

---

*Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices.* GAO-08-240. Washington, D.C.: April 25, 2008.

*Supply Chain Security: Examinations of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed.* GAO-08-187. Washington, D.C.: January 25, 2008.

*Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System.* GAO-06-591T. Washington, D.C.: March 30, 2006.

*Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts.* GAO-05-557. Washington, D.C.: April 26, 2005.

*Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security.* GAO-05-404. Washington, D.C.: March 11, 2005.

*Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors.* GAO-03-770. Washington, D.C.: July 25, 2003.

<b>GAO's Mission</b>	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
<b>Obtaining Copies of GAO Reports and Testimony</b>	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website ( <a href="http://www.gao.gov">http://www.gao.gov</a> ). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <a href="http://www.gao.gov">http://www.gao.gov</a> and select "E-mail Updates."
<b>Order by Phone</b>	<p>The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <a href="http://www.gao.gov/ordering.htm">http://www.gao.gov/ordering.htm</a>.</p> <p>Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.</p> <p>Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.</p>
<b>Connect with GAO</b>	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at <a href="http://www.gao.gov">www.gao.gov</a> .
<b>To Report Fraud, Waste, and Abuse in Federal Programs</b>	<p>Contact:</p> <p>Website: <a href="http://www.gao.gov/fraudnet/fraudnet.htm">http://www.gao.gov/fraudnet/fraudnet.htm</a>  E-mail: <a href="mailto:fraudnet@gao.gov">fraudnet@gao.gov</a>  Automated answering system: (800) 424-5454 or (202) 512-7470</p>
<b>Congressional Relations</b>	Katherine Siggerud, Managing Director, <a href="mailto:siggerudk@gao.gov">siggerudk@gao.gov</a> , (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
<b>Public Affairs</b>	Chuck Young, Managing Director, <a href="mailto:youngc1@gao.gov">youngc1@gao.gov</a> , (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548



Please Print on Recycled Paper.

Testimony

The Honorable Janice Hahn  
Congresswoman  
44<sup>th</sup> Congressional District of California

Before the

Committee on Homeland Security and Government Affairs  
United States Senate

Evaluating Port Security: Progress Made and Challenges Ahead

June 4, 2014

Thank you, Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. While I am unable to attend this hearing in person due to the House adjourning for a district work period, I appreciate the opportunity to share my comments with the Committee on the very important topic of evaluating port security. I specifically want to thank Ranking Member Coburn who committed to me that this hearing would be held, and I am grateful for all the work the Homeland Security and Government Affairs Committee does in protecting our nation's most important points of entry.

We have a responsibility as Members of Congress to ensure all gateways into our country are safe and secure, and I look forward to working with my colleagues in the Senate and House to close the gaps that exist in our nation's port security.

On September 11, 2001 our nation was caught unprepared for a devastating attack from terrorists determined to change our way of life. The attack forever changed the way we operate, but failed to shake our resolve. In the following years, we saw the creation of the Department of Homeland Security, new safety procedures at our country's ports of entry, and a more vigilant approach to securing our homeland. However, while we saw a massive shift in air travel safety procedures preventing countless terrorist attacks, some sectors of our transportation network - such as our maritime ports - have lagged behind in security procedures.

I represent the Port of Los Angeles, which is part of the largest port complex in the United States. In fact, my backyard and the community I live in overlook the flow of goods entering and leaving our country. Threats to our ports mean threats to our port communities. It keeps me up at night thinking of the damage to our infrastructure and economy an attack would cause.

When I arrived in Congress I saw a lack of understanding and focus on our economic gateways, which drove me to found the Congressional Ports Caucus with my colleague from Texas, Congressman Ted Poe. The Congressional Ports is 88 members strong. The Caucus includes members from around the country who represent ports of all sizes, with members from the East,

Midwest, Gulf Coast, Great Lakes, and West. In the past 3 years, we've been actively advocating for additional port security funding and improvements to our maritime ports.

Due to the nature of the threat from 9/11 attacks, we have greatly increased our aviation security to address post-9/11 threats. As a result, potential terrorists likely will turn their attention to other targets and transportation modes. Our ports are the most logical of such alternative targets, but I do not believe we have done enough to upgrade our port security in a manner commensurate with the increased threat. Ships make 50,000 calls a year on U.S. ports, carrying two billion tons of freight and 134 million passengers. Each day our ports move both imports and exports totaling some \$3.8 billion worth of goods through all 50 states. Additionally, ports move 99.4 percent of overseas cargo volume by weight and generate \$3.95 trillion in international trade. Leaving our maritime ports unprepared for an ever-changing landscape of dangers could place our entire economy at risk.

According to a recent CRS report, a 10- to 20-kiloton weapon detonated in a major seaport would kill 50,000 to 1 million people and would result in direct property damage of \$50 to \$500 billion, losses due to trade disruption of \$100 billion to \$200 billion, and indirect costs of \$300 billion to \$1.2 trillion. When our west coast ports were closed in 2002 due to a strike, it cost the economy \$1 billion per day, which represented 4% of our economy. Imagine if we needed to shut all of the United States ports – the result would drive us into depression.

Congress attempted to address some of these issues by passing the Maritime Transportation Security Act of 2002, the Safe Port Act in 2006, and the 9/11 Commission Act of 2007, which specifically required that 100% of the cargo coming into our ports be scanned by the summer of 2014. Unfortunately, DHS has made very little progress in achieving this goal and does not plan to implement it. In fact, we have recently learned that DHS has only been scanning as little as 3% of all the cargo imported into the United States.

While the feasibility of scanning 100% of incoming cargo may be a legitimate concern, there certainly needs to be improvement from where we are now. An attack on the Port of Los Angeles/Long Beach complex, for example, would cost billions to the regional economy, put thousands of port employees out of work and cause the demise of hundreds of local businesses.

However cargo screening is just the tip of the iceberg. Our ports are subject to many more risks – both known and unknown, and our federal actions towards port security have been lacking, to say the least. To identify what risks are present for our nation's maritime ports, I was proud to author and pass through the United States House of Representatives H.R. 4005 "Gauging American Port Security Act" or GAPS Act in the 112<sup>th</sup> Congress. Unfortunately, this bill never saw the light of day in the United States Senate. The issues that exist in our maritime security have not been solved, but rather only grown in the past two years.

Following the passage of my legislation, the Brookings Institution released a report highlighting additional gaps in our port security measures, specifically a major deficiency in preparing for cyber-security threats. The July 3, 2013 Brookings report titled *The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities* states that "a cyber disruption affecting energy supplies would likely send a shockwave through the U.S. and global economy."

Our ports lack proper funding to prepare themselves for a potential attack, and should funding be provided, lack a general knowledge of how to institute an effective plan to combat cyber threats. Further, ports must operate in direct competition with each other, with razor thin profit margins, leaving many ports inclined to side with cost savings over security improvements. These gateways for our country need guidance and leadership from the United States Congress in formulating a uniform security improvement plan.

I am working with my House colleagues to once again pass my GAPS Act in the 113<sup>th</sup> Congress, and I urge my Senate colleagues to do the same.

The risks that exist at our ports are real, and would have wide reaching impacts on every sector of the United States economy. For those reasons, I thank the Committee for allowing me the opportunity to share my thoughts on port security. I stand ready to work with my colleagues in the Senate and House to modernize how we manage port security, and thank you for holding this important hearing today.



Alliance of the Ports of Canada, the Caribbean, Latin America and the United States

**AMERICAN ASSOCIATION OF PORT AUTHORITIES**  
1010 Duke Street • Alexandria, VA 22314  
Phone: (703) 684-5700 • Fax: (703) 684-6321

**Kurt J. Nagle, President**  
**On behalf of the American Association of Port Authorities**  
**Submitted for the Record of the**  
**The United States Senate**  
**Hearing: *Evaluation of Port Security: Progress Made and Challenges Ahead***  
**June 4, 2014**

The American Association of Port Authorities (AAPA) is submitting this testimony for the hearing record on the *Evaluation of Port Security: Progress Made and Challenges Ahead*. AAPA represents more than 130 public port authorities in the United States, Canada, the Caribbean and Latin America. These comments represent those of U.S. ports members.

Since the tragic day of September 11, 2001, America's seaports have been partners with the federal government and our local communities in developing and implementing a comprehensive port security program. Seaports are international border and gateways to America, and the federal government has a clear Constitutional responsibility to protect them. Safe and secure seaports are fundamental to protecting our borders and moving goods.

My comments focus on port security grants, scanning equipment and requirements, staffing and facility design requirement and the Transportation Worker Identification Credential (TWIC) program. AAPA has also voiced support for Rep. Janice Hahn's GAPS Act, H.R. 1535, to study future needs of port security.

**Port Security Grants**

The Port Security Grant Program (PSGP) continues to be an indispensable tool for U.S. ports. This program allows ports to serve as strong partners with the Department of Homeland Security in our ongoing efforts to harden security and protect our homeland. In order for our country to be safe, AAPA believes that all ports must continue to be eligible for port security grants, which serve as aids in protecting this country from terrorist and other criminal attacks. We all must have the commitment and resources to keep our country safe.

In the decade since 9/11, a key component of our nation's effort to tighten the security of seaports has been the Port Security Grant Program, currently managed by the Federal Emergency Management Agency (FEMA). Port Security Grant funds have helped port facilities and port areas to strengthen facility security and work in partnership with other agencies to enhance the security of the region. Port Security Grant funding has been used to procure equipment such as vessels and vehicles, install detection systems such as cameras and sensors, and provide equipment maintenance for the systems recently installed. Each port may have different security needs, but the commitment and needed outcomes are the same. Securing our ports is an ongoing effort.

AAPA is concerned about recent dramatic cuts to the program, which originally had been funded at the authorized level of \$400 million but now only receives \$100 million. Additionally, FEMA changed the period of performance to a strict two-year period which has resulted in a focus on easy-to-do projects and easy-to-purchase equipment rather than looking at the highest risk needs. AAPA strongly urges FEMA to return to the system in which grants have a three-year term with a two-year extension allowed.

AAPA would also like to address the Administration's National Preparedness Grant Program proposal. This proposal was drafted several years ago, but just recently the Administration sent over the proposal in the form of an authorization bill to Congress. The proposed bill outlines how various programs would be changed and details how the new program would work. AAPA has been engaged in discussions with FEMA over the last few years and our concerns still have not been properly addressed in the proposal.

AAPA's first concern with the Administration's National Preparedness Grant Program is that it calls for funding of the program to be determined at the state level, along with other homeland security grants. Essentially, this amounts to block grant funding for our national security needs. This model may have worked for other agencies such as HUD's Community Development Block Grant Program (CDBG), but when dealing with security risks, continuity, details and coordination with other federal agencies are vital and are in the nation's interest. AAPA strongly believes the Port Security Grant Program must be maintained at the federal level. Seaports are international borders and must comply with numerous federal regulations including those instituted by TSA, Customs and Border Protection, the Department of Agriculture and the U.S. Coast Guard. Port Security Grants are often used to help facilities address these federal mandates. Often states are unfamiliar with federal requirements and do not have the expertise to determine risks to these international seaport borders. AAPA has fought hard to ensure the program makes all seaports that serve as international borders eligible for the program. FEMA has provided grants to seaports at all levels in order to ensure that our nation does not have an exposed soft-underbelly of underprotected ports. We must not allow for a weak spot that terrorists can capitalize on. There is no mandate in the Administration's proposal requiring states even to fund port security and it is likely to result in some ports not getting funding for needed projects. Additionally, other grant and oversight programs such as border security (land, air and maritime) are a national, not a state, responsibility. AAPA believes that weakening our national seaports would also weaken other national infrastructure resources such as airports and borders.

The Maritime Transportation Security Act, passed soon after 9/11, and the subsequent SAFE Port Act carefully laid out a system to identify risks and fund projects accordingly, with both national and local input. FEMA, with input from the U.S. Coast Guard and national intelligence information, determines which ports should be in each risk category while local area committees develop plans to decrease these risks. State officials are invited to sit on these local area committees, but the responsibility to determine who gets a grant resides with the Secretary of the Department of Homeland Security, based on evaluation from the local and national U.S. Coast Guard offices, FEMA and other federal partners. This is where AAPA believes the authority to determine grants should continue to reside – at the federal level, where the expertise exists and the national security needs as well as local needs can best be addressed.

Secondly, the Administration's proposal expands the grants to all hazards, and simultaneously cuts overall funding. With the expansion of the grants to all hazards, more projects will be eligible, resulting in less funding for port security. This would not be a sustainable model to keep our seaports, communities and nation safe. In addition to increased eligibility, the proposal calls for a significant decrease in funding overall. Currently, Port Security Grants are only funded at 25 percent of the authorized level of \$400 million. Merging the program into other homeland security grants is likely to result in a substantial decrease.

Finally, the separation of Port Security Grant funding served to highlight the need to focus on a component of the nation's critical infrastructure and international border that was largely ignored prior to the tragic events on 9/11. We fear that this focus will be lost if the Port Security Grant Program does not remain separate and fails to continue to grow to meet emerging security needs.

#### **Financial Responsibility for Scanning**

Ports have worked closely with Customs and Border Protection (CBP) to carry out 2002 and 2007 laws mandating that cargo scanning take place to prevent nuclear or other radiological devices from entering the United States. CBP has placed radiation portal monitors (RPM) in all container ports but problems exist related to a plan to maintain and replace RPMs and other scanning equipment.

Evidence collected by the DHS Office of Inspector General shows that Customs and Border Protection and the Domestic Nuclear Detection Office do not have a plan for continuing maintenance, replacement, or funding for these machines (e.g., Radiation Portal Monitors, VACIS, etc.). CBP has reached out to ports and terminal operators asking them to pay for these expensive systems. AAPA believes strongly that ports and terminal operators should not be required to fund this security program, initiated by the federal government in order to secure international borders.

AAPA requests that DHS conduct a study on how the agency intends to pay for the future use of scanning equipment including needed changes due to port facility expansion or reconfiguration and for disposition of current scanning machines reaching the ends of their useful lives. CBP also needs to gather information on port expansions to determine future needs and costs. Additionally, DHS should fund the On-Dock Rail (ODR) radiation detection program, which has

already undergone successful testing to efficiently scan containers moving directly to rail from ships. Direct On-Dock Rail scanning would help improve cargo moving efficiency at ports.

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

AAPA continues to work with DHS on implementing the Transportation Worker Identification Credential (TWIC) program, including monitoring and commenting on U.S. Coast Guard (USCG) regulations for facility compliance with TWIC. AAPA would like to see a TWIC rule finalized.

AAPA has concerns with the USCG's proposed TWIC reader rule for several reasons: the criteria used for determining which ports are subject to the reader requirement, the inflexibility of the risk analysis methodology, and the lack of tailoring reader requirements for the individual circumstances of each port or facility. Most facilities under the proposal rule would not require a TWIC. The question then becomes why have such a costly card that few will use other than as a flash pass. AAPA believes more robust use of card readers would result in increased security. The current proposal only requires facilities that handle Certain Dangerous Cargos and high passenger volumes to use readers. AAPA believes this requirement for readers is too narrow.

Finally, the delay in the final USCG regulations related to TWIC reader requirements has resulted in reprogramming of some TWIC grants to other priorities. Once the new rules are finalized, DHS should make TWIC grants a priority.

#### **CBP Staffing and Facility Design Needs**

Recently, Congress provided CBP with 2000 new officers to address increasing needs including those at seaports. AAPA would like to ensure that CBP has studied the needs of the seaport including projected changes in trade patterns and increased trade, and incorporate these current and future needs into its staffing plan. Emphasis should be placed on CBP availability to meet demands of trade without any additional cost to the trade to pay for overtime. Flexibility is often missing to accommodate extended gates to address temporary or permanent changes in trade volumes. CBP is fee-based, but often will only provide flexibility if facilities agree to pay for overtime. There also is inconsistent policy with some ports getting 24x7 CBP service and others being asked to pay for overtime if additional officers are needed. Since this is a fee based system, CBP should be able to provide these services without charging a facility over time.

CBP also needs to provide officers and flexible low-cost facilities for the changing cruise market to provide needed officers, especially in seasonal areas as well as areas of growth. Flexibility is key to the cruise market. CBP's design standards, especially in the cruise area, also need to be more flexible and should not be so costly or over-built that they result in a large financial burden to seaports.

**100% Scanning Mandate**

AAPA has also joined with 70 other organization to support DHS's recent two-year waiver of the federal requirement that 100% of containers be scanned overseas. DHS has carefully reviewed the requirement that all cargo be scanned overseas before being loaded onto a U.S.-bound ship and has concluded that this mandate is unworkable. We ask Congress to look at the long-term viability of this mandate.

**Conclusion**

Thank you again for accepting AAPA's written testimony for this very important hearing. Key ways forward include:

- passing the GAPS Act, Rep. Hahn's H.R. 1535, to study gaps in our nation's port security and make recommendations for the future;
- Keeping the Port Security Grants at the federal level, expand the grant performance to 3-5 years and provide a level of funding that will allow us to continue to make progress;
- Provide the needed funding to CBP to study, maintain, replace and meet future trade needs for scanning technology;
- Require CBP's staffing and design standards to meet the needs of the industry. Encourage CBP to more fully understand the staffing and facility requirements at both cruise and cargo ports; and
- Require TWIC reader requirements to be broader than those currently proposed.

AAPA looks forward to continuing to work with the Homeland Security and Governmental Affairs Committee on ensuring that our seaport security challenges are being met. Please continue to consider us a partner and a resource.

###

*Before the*

**United States Senate**

**Committee on Homeland Security and  
Governmental Affairs**

**Statement of**

**American Trucking Associations, Inc.**

**For the Hearing on**

*Evaluating Port Security: Progress Made and Challenges Ahead*

**JUNE 4, 2014**



**AMERICAN  
TRUCKING  
ASSOCIATIONS**

950 N. Glebe Road  
Arlington, VA 22203  
703-838-1996

### 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 30,000 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.<sup>1</sup> 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 stated at several Congressional hearings, 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, including at maritime port facilities. 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. ATA believes that the Transportation Worker Identification Credential (TWIC), which provides a credentialing/background check as well as a physical access control security mechanism at regulated port facilities, can be such a program if implemented and utilized in an appropriate manner.

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 costs to drivers and companies of these separate STAs and credentials is almost \$300 in fees alone, not including the costs associated with drivers' lost wages and fuel costs to travel to and from enrollment centers, and the aggravation of providing fingerprints multiple times for each program to perform the same background check.

The combined costs to the trucking industry of the TWIC and HME screenings have already surpassed the \$200 million in fees alone<sup>2</sup>, not including lost wages for time off work to undergo the application and fingerprinting processes. Using TSA's own numbers there were approximately 2.7 million commercial drivers with HMEs in 2004<sup>3</sup>. Today, after having already completed a full cycle of HME renewals on the truck driver population, there are approximately

<sup>1</sup> American Trucking Associations, *American Trucking Trends 2011* (March 2011).

<sup>2</sup> 1.5 million commercial drivers with HMEs x \$89 = \$133.5 million, plus 500,000 drivers x \$132.50 = \$66.3 million, for a total of \$178.5 million. The present STA costs described above have only been in place for about one year.

<sup>3</sup> 69 *Federal Register* at 68739 (November 24, 2004)

1.5 million commercial drivers with HMEs.<sup>4</sup> The drop in the population of drivers with HMEs is not a result of applicants being disqualified during the screening process – less than 1 percent of applicants have received final disqualification letters and those have mostly been issued because the drivers did not understand and avail themselves of the screening program's appeal and waiver process.<sup>5</sup>

ATA believes that the reduced number of HME holders is due primarily to the costs and the burden on commercial drivers of the fingerprinting and application process for getting an HME. Some trucking companies with a small percentage of hazardous materials loads have even stopped transporting such cargo to avoid burdening their drivers with the HME screening, especially considering that the industry faces a continuing shortage of qualified commercial drivers. Requirements that increase the burden of entry for drivers to our industry, such as redundant background checks, compound the challenge for companies to hire and add new drivers to their payrolls.

Over a decade ago, Admiral James Loy, then the second most senior official at the Transportation Security Administration (TSA), described the TWIC concept as follows:

*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.<sup>6</sup>*

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. With over half a million known commercial drivers holding valid TWICs today, the trucking industry is heavily invested in the TWIC program<sup>7</sup>. The 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 (DHS) 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;

<sup>4</sup> Data provided by TSA at meetings of Highway Motor Carrier Government-Sector Coordinating Council. 25,000 commercial drivers underwent HME screenings in five years of the program: 60 months x 25,000 = 1.5 million.

<sup>5</sup> TSA has shared with ATA staff that applicants that have received final disqualifications letters, for both the TWIC and HME programs, represent less than one percent.

<sup>6</sup> 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.

<sup>7</sup> Data provided by TWIC Program Office, Office of Intelligence and Analysis, TSA, as of May 7, 2014.

- The failure to expand TWIC's utilization to satisfy other federal STA regulatory requirements, including identical STA programs within TSA;
- The past lack of TWIC enrollment facilities nationwide to facilitate the enrollment of transportation workers who live far from either coast, an issue that is being addressed by the new contractor;
- The failure to implement the TWIC rule 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 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 inefficient. Because of this, ATA supports the TWIC as the potential single credential and STA that can demonstrate and provide compliance with multiple programs and regulations.

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 a report issued a year ago regarding the TWIC card reader pilot results<sup>8</sup>, 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

<sup>8</sup> U.S. Government Accountability Office; *Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to be Reassessed*; May 2013

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.

The TWIC reader Notice of Proposed Rulemaking (NPRM) is critical in fulfilling a key goal of the overall TWIC program to allow for the verification and authentication of the credential, as well as matching the credential to the cardholder's identity. ATA supports the implementation of the TWIC readers in order to not only improve security, but to also improve throughput at maritime facilities for commercial vehicles. ATA raised the following issues to the NPRM as recommendations and concerns that USCG and TSA should address to ensure a uniform and improved implementation of the TWIC reader rule:

- Industry supports a risk-based approach in implementing security regulations, but the use of TWIC readers should be expanded beyond Group A, rather than continuing to utilize expensive TWIC smart cards as "flash-passes" for visuals inspections;
- TSA and USCG must develop specific recordkeeping requirements for information collected and stored by MTSA-regulated facilities from TWIC cardholders to protect the privacy and security of such data;
- Establish uniform TWIC reader standards at all facilities and establish a true "consistent user experience" to minimize any potential problems with variances in equipment, additional training needs, and overall user difficulties.

ATA supported the following specific proposals within the NPRM:

- Establishing alternative entry procedures when readers malfunction or when cards are lost or damaged, and providing the Captain of the Port greater flexibility in extending such periods if necessary;
- Not requiring the use of the TWIC PIN at readers when entering a secure area of a facility, which would significantly increase processing times;
- Establishing preemption to avoid duplicative processes by State and local authorities.

With the appropriate vision within DHS 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 some sectors within government 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. 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. Again, the 2.4 million transportation workers in possession of a TWIC, including over 500,000 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 valuable resources and time to obtain the credential.

ATA urges the Senate's Homeland Security and Governmental Affairs Committee to:

- 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 and secure facilities;
- Authorize and mandate the use of the TWIC for compliance with equivalent STA programs, such as the HME program;
- 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 standalone 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 reader rule, after careful consideration of affected stakeholder comments and recommendations, to fully leverage the technology embedded in the TWIC and to establish uniform, secure, and efficient access procedures at MTSA-regulated facilities.

ATA appreciates the opportunity to offer this written statement for consideration by the Senate's Homeland Security and Governmental Affairs Committee. We also look forward to providing any additional information you may request to improve the security of our transportation system.

ATA Contact:

Martin Rojas  
Vice President, Security & Operations  
American Trucking Associations (ATA)  
950 N. Glebe Road, #200  
Arlington, VA 22203  
T 703-838-7950



STATEMENT OF COLLEEN M. KELLEY  
NATIONAL PRESIDENT  
NATIONAL TREASURY EMPLOYEES UNION  
ON EVALUATING PORT SECURITY:  
PROGRESS MADE AND CHALLENGES AHEAD  
BEFORE THE COMMITTEE ON HOMELAND SECURITY  
AND GOVERNMENTAL AFFAIRS  
U.S. SENATE

June 4, 2014

Chairman Carper, Ranking Member Coburn, distinguished members of the Committee; thank you for the opportunity to provide this testimony. As President of the National Treasury Employees Union (NTEU), I have the honor of leading a union that represents over 24,000 Customs and Border Protection (CBP) Officers and trade enforcement specialists stationed at 329 land, sea and air ports of entry (POEs) across the United States.

Understaffed ports lead to long delays in our commercial lanes as cargo waits to enter U.S. commerce. NTEU strongly supported provisions in the FY 2014 Omnibus Appropriations bill that provided funding to hire an additional 2000 new CBP Officers by the end of FY 2015 at the air, sea and land ports of entry. NTEU also strongly supports the Administration's legislative proposal in its FY 2015 budget request to fund the hiring of an additional 2000 CBP Officers--bringing the total number of CBP Officers to 25,775—through an increase in customs and immigration user fees. This increase is supported by CBP's FY 2014 Resource Optimization at Ports of Entry Report to Congress which includes the results of the Workforce Staffing Model that identifies a pre-Omnibus need for 3,811 new CBP Officers. **It is important that the Committee authorize funding for these additional 2000 CBP Officers in FY 2015 and beyond.**

For years, NTEU has maintained that delays at the ports result in real losses to the U.S. economy. According to the U.S. Department of the Treasury, more than 50 million Americans work for companies that engage in international trade and, according to a recent University of Southern California study, "The Impact on the Economy of Changes in Wait Times at the Ports of Entry", dated April 4, 2013, for every 1,000 CBP Officers added, the U.S. can increase its gross domestic product by \$2 billion, which equates to 33 new private sector jobs per CBP Officer added.

NTEU strongly supports the increase in the immigration and customs user fees by \$2.00 each to fund the hiring of an additional 2000 CBP Officers in FY 2015, but recognize that this

increase may not be approved by Congress. CBP collects user fees to recover certain costs incurred for processing, among other things, air and sea passengers, and various private and commercial land, sea, air, and rail carriers and shipments. The source of these user fees are commercial vessels, commercial vehicles, rail cars, private aircraft, private vessels, air passengers, sea passengers, cruise vessel passengers, dutiable mail, customs brokers and barge/bulk carriers. These fees are deposited into the Customs User Fee Account. Customs User Fees are designated by statute to pay for services provided to the user, such as inspectional overtime for passenger and commercial vehicle inspection during overtime shift hours. User fees have not been increased in years and some of these user fees cover only a portion of recoverable fee-related costs. In 2010, CBP collected a total of \$13.7 million in Commercial Vehicle user fees, but the actual cost of Commercial Vehicle inspections in FY 2010 was over \$113.7 million—a \$100 million shortfall.

Increasing the immigration inspection user fee by \$2 will allow CBP to better align air passenger inspection fee revenue with the costs of providing immigration inspection services. According to the Government Accountability Office (GAO) (GAO-12-464T, page 11), fee collections available to ICE and CBP to pay for costs incurred in providing immigration inspection services totaled about \$600 million in FY 2010, however, “air passenger immigration fees collections did not fully cover CBP’s costs in FY 2009 and FY 2010.”

Despite an increase in appropriated funding in fiscal years 2014 and 2015 for an additional 2000 CBP Officers, **CBP will still face staffing shortages in FY 2015 and beyond.** If Congress is serious about job creation, then Congress should support enactment of legislation that increases the IUF and COBRA fees by \$2.00 each and adjust both fees annually to inflation. **If Congress does not enact the user fee increases requested, the needed staffing enhancement must be funded by discretionary appropriations. This Committee should authorize appropriations to address the ongoing CBP Officer staffing shortages as identified by CBP’s Workforce Staffing Model, as well as shortages of CBP staff in CBP’s other vital agriculture and trade inspection and compliance missions.**

#### **CBP STAFFING AT SEA PORTS OF ENTRY AND THE SEQUESTER**

**NTEU strongly urges Congress to end the sequester.** Without enactment of the Omnibus appropriations bill, the sequester would have severely restricted CBP’s ability to address critical staffing needs at the ports of entry in fiscal years 2014 and 2015. If Congress doesn’t reverse the Budget Control Act, another round of sequestration will be devastating to CBP—requiring furloughs and hiring freezes, eliminating overtime, reducing services, increasing wait times for trade and travel and jeopardizing national security.

According to a recent report by the GAO on the 2013 Sequestration (GAO-14-452, May 2014, page 21), “OFO officials from the Houston, Los Angeles, and New York field offices cited effects on cargo operations resulting from sequestration. Specifically, to ensure that international air passenger wait times were kept to a minimum in fiscal year 2013, these three

field offices chose to shift officers who typically inspected cargo to the air passenger environment.”

CBP inspection of passengers and crewmembers in a seaport environment differs significantly from airport or land border inspection. Most vessels inspected are cargo vessels, with only crewmembers on board. Passenger vessels are predominantly cruise ships, with most passengers beginning and ending their trips in the United States. As stipulated in the CBP Directive on national commercial vessel entry and boarding policy:

**2.2 Passenger/Crew Inspection.** By law, upon arrival, CBP must inspect all persons arriving into the United States from foreign ports or places. CBP Officers will board all commercial vessels arriving from foreign ports or places to determine the admissibility of all persons on board. As a point of clarification, under the Immigration and Nationality Act, all persons are inspected for a determination of admissibility; U.S. citizens are examined for verification of citizenship. In addition, CBP Officers will board commercial vessels, as necessary and consistent with sound risk management principles, traveling coastwise that carry crewmembers who have been refused permission to land and ordered detained-on-board to ensure compliance with the order.

Restrictions on overtime and reassignment of CBP Officers from cargo clearance to passenger processing due to both staffing shortages and budget constraints, as noted in the May 2014 GAO report, vessel inspection and clearance of cargo and crew at the seaports may be delayed up to a day. Without immediate dockside inspection, it is possible that unknown persons can board these vessels and crew can disembark and offload cargo, all prior to receiving inspection and clearance from a CBP Officer. The possibility of cargo being unloaded prior to inspection increases the risk that contraband and improperly labeled cargo will enter the United States. Once the cargo is off-loaded, it can be transported anywhere in the United States without further inspection. Also, it is possible that crew members who have security issues may disembark or may use the opportunity to illegally enter the United States--a potential threat to national security.

Budget constraints that limit CBP Officer overtime usage and result in delayed dockside inspection and clearance, are also costly to the commercial shipping industry in both fuel and turnaround costs. Often these delayed inspection costs are passed on to the consumer in higher prices of shipped goods.

For these reasons, NTEU urges Congress to end the sequester and support raising customs and immigration user fees that pay for CBP Officer and Agriculture Specialist overtime, to achieve full cost recovery of overtime services and address CBP Officer staffing shortages.

**AGRICULTURE SPECIALIST STAFFING SHORTAGE AT SEA PORTS OF ENTRY**

CBP employees at the ports also perform agriculture inspections to prevent the entry of animal and plant pests or diseases. The Port of Wilmington, Delaware is the top North American port for imports of fresh fruit, bananas, and juice concentrate, and maintains the largest dock-side cold storage facility. U.S. agriculture sector is a crucial component of the American economy, generating over \$1 trillion in annual economic activity. According to the United States Department of Agriculture (USDA), foreign pests and diseases cost the American economy tens of billions of dollars annually. Failure to detect and intercept these non-native pests and diseases imposes serious economic and social costs on all Americans. **Staffing shortages and lack of mission priority for the critical work performed by CBP Agriculture Specialists and CBP Technicians assigned to the ports is a continuing threat to the U.S. economy.**

To address CBP Agriculture Specialist staffing shortages at the ports of entry, NTEU supports funding to hire additional CBP Agriculture Specialists. We also support GAO recommendations aimed at more fully aligning Agriculture Quality Inspection (AQI) fee revenue with program costs (see GAO-13-268). According to GAO, in fiscal year 2011, CBP incurred 81 percent of total AQI program costs, but received only 60 percent of fee revenues; whereas the Animal, Plant Health Inspection Service (APHIS) incurred 19 percent of program costs but retained 36 percent of the revenues. In other words, APHIS covers all its AQI costs with AQI fee revenues, while CBP does not. AQI user fees fund only 62 percent of agriculture inspection costs with a gap of \$325 million between costs and revenue. To bridge the resulting gap, CBP uses its annual appropriation.

NTEU supports CBP's efforts to establish an Agriculture Specialist Resource Allocation Model to ensure adequate CBP Agriculture Specialist staffing at the POEs. Release of the Agriculture Specialist Workforce Staffing Model, initially due at the end of September 2013, however, has been postponed. NTEU has learned that the Model, when released, will show a significant staffing shortage at the ports and a need to hire a significant number of additional CBP Agriculture Specialists. **NTEU requests that the Committee authorize funding to hire additional CBP Agriculture Specialists as specified in the forthcoming workforce staffing model.**

**RECOMMENDATIONS**

Additional CBP staff must be authorized to ensure security and mitigate prolonged wait times for both trade and travel at our nation's ports of entry. Therefore, **NTEU urges the Committee to:**

- **End the sequester;**
- **Authorize the hiring of an additional 2000 CBP Officers--bringing the total staffing number to 25,775;**

- **Authorize the hiring of additional agriculture inspection and trade enforcement personnel to adequately address increased agriculture and commercial trade volumes.**

The more than 24,000 CBP employees represented by NTEU are proud of their part in keeping our country free from terrorism, our neighborhoods safe from drugs and our economy safe from illegal trade, while ensuring that legal trade and travelers move expeditiously through our air, sea and land ports. These men and women are deserving of more resources to perform their jobs better and more efficiently.

Thank you for the opportunity to submit this testimony to the Committee on their behalf.

## Securing America's Ports

Henry H. Willis

RAND Office of External Affairs

CT-410

June 2014

Testimony submitted before the Senate Homeland Security and Governmental Affairs Committee on June 4, 2014

This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.



Published 2014 by the RAND Corporation  
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138  
1200 South Hayes Street, Arlington, VA 22202-5050  
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665  
RAND URL: <http://www.rand.org/>  
To order RAND documents or to obtain additional information, contact  
Distribution Services: Telephone: (310) 451-7002;  
Email: [order@rand.org](mailto:order@rand.org)

Henry H. Willis<sup>1</sup>  
The RAND Corporation

*Securing America's Ports*<sup>2</sup>

Before the Committee on Homeland Security and Governmental Affairs  
United States Senate

June 4, 2014

Chairman Carper, Ranking Member Coburn, and members of the Committee, thank you for inviting me to submit testimony for this hearing.

As this committee considers the issue of port security, I will point out three ways we can make America's ports more secure:

- Improve the evaluation of port security programs.
- Increase the reliance on local risk assessments when awarding port security grants.
- Reconsider the 100% container inspection mandate.

**The importance of securing America's ports**

America's ports play a vital role in the nation's economy. Each year approximately \$500 billion in containerized imports and \$200 billion in containerized exports transit our ports as more than 12 million containers are loaded onto ships.<sup>3</sup> In addition, U.S. ports enable the efficient shipment of non-containerized exports such as oil and grain.

This productivity is the result of complex cooperation among many sectors. Transportation firms physically bring freight to and from ports via water, road and rail. Local law enforcement, the U.S. Coast Guard, and U.S. Customs ensure trade occurs safely and in accordance with U.S. laws. Banks, brokers, and freight consolidators make sure that shippers needing goods can contract with manufacturers or suppliers who have them and carriers who can transit them. These interactions make the freight supply chain of the U.S. one of the most efficient and rapid in the world.<sup>4</sup>

---

<sup>1</sup> The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

<sup>2</sup> This testimony is available for free download at <http://www.rand.org/pubs/testimonies/CT410.html>.

<sup>3</sup> Bureau of Transportation Statistics (2011). *America's Container Ports: Linking Markets at Home and Abroad*. US Department of Transportation, Washington, DC.

<sup>4</sup> Willis, H. H., D. S. Ortiz (2004). *Evaluating the Security of the Global Containerized Supply Chain*. TR-214-RC, RAND Corporation, Santa Monica, CA.

The scale and the complexity of ports draw attention to their vulnerability to terrorism and natural disasters. If targeted by an attack or affected by a disaster, resulting disruptions at ports could lead to cascading economic damages totaling billions of dollars.<sup>5</sup> The difficulty of thoroughly inspecting containers leads criminals to use them as a common means of smuggling. Thus, policymakers and security analysts point out that terrorists might also try to use this mode of transit to bring nuclear weapons or other materials into the country.<sup>6</sup>

The response to perceived vulnerabilities of U.S. ports has been the accretion of a layered system of defenses to secure America's ports. The Maritime Transportation Security Act implemented requirements to make vessels and port facilities more secure. The Transportation Worker Identification Credential (known as TWIC) was developed to reduce insider threats associated with freight transportation operations. U.S. Customs introduced advanced manifest notification rules to enable capabilities to screen incoming freight in advance of it being loaded on ships bound for the U.S. Secure trade lanes, such as the Customs-Trade Partnership Against Terrorism, were implemented to reduce the impact of new security measures on the efficiency of trade. Requirements were legislated for the use of radiological detection and non-invasive imaging to scan containers and equipment. These technologies have now been installed at ports around the world to counter nuclear smuggling threats.<sup>7</sup>

As these security programs have matured over the last decade, two programs warrant special attention at this hearing: the Port Security Grant Program and the SAFE Ports Act requirement for 100% scanning of all containers imported into the U.S. before they are loaded aboard a ship. Funding for improving port security has declined from \$389 million in 2008 to \$100 million in 2014.<sup>8</sup> U.S. Customs and Border Protection continues to implement risk-based container screening and scanning but is still held accountable for the 100% scanning requirement. These fiscal and operational realities make it an opportune time to ask three questions about the state of port security:

- What has more than a decade of investments in improving port security accomplished?
- Are the current priorities for port security grant programs correct?
- Should the 100% scanning requirement be implemented?

**What have investments in improving port security accomplished?**

Unfortunately, the answer is we don't really know.

<sup>5</sup> Adam Rose and Dan Wei (2013). Estimating the economic consequences of a port shutdown: The special role of Resilience. *Economic Systems Research*, Vol. 25, No. 2, 212–232.

<sup>6</sup> GAO (2006). *Combating Nuclear Smuggling*. GAO-06-389, Washington, DC.

<sup>7</sup> Willis, H. H., D. S. Ortiz (2004). *Evaluating the Security of the Global Containerized Supply Chain*. TR-214-RC, RAND Corporation, Santa Monica, CA.

<sup>8</sup> These figures are in nominal dollars, thus the decline in funding would be even greater in constant year dollars.

The latest approaches to measuring security and preparedness apply performance logic models to explain how funding and resources make a difference.<sup>9</sup> Such approaches help us distinguish:

- Inputs – funding, people, facilities and equipment that are available to improve security.
- Capacities – how inputs are organized to support functions that improve security.
- Capabilities – what tasks can be performed to improve security.
- Outcomes – What is ultimately achieved as a goal.

Most attempts to describe how grant programs have improved security describe what inputs and capacities have been developed. For example, communities have developed security and emergency management plans. They have purchased and stockpiled materials to be used during a disaster and installed security equipment, such as guards, gates and cameras, to make ports less vulnerable. They have upgraded communications equipment and established mutual support agreements with neighboring jurisdictions to improve coordination during a response. They have even trained employees and volunteers on how to respond when an event happens. Radiological detection equipment has been installed in ports around the world. By measures like these, funding for port security, or for that matter broader counter-terrorism and preparedness, has clearly made a difference.

However, these measures describe inputs and capacities. Having capacity is not the same as having the capability to respond. The difference between capacity and capability is the difference between having a bicycle and being able to ride it. Thus, while it is easy to identify how grant funding was spent, it is challenging to determine what difference the change makes.

Ultimately, program evaluation should address outcomes. For preparedness grants the ultimate outcome, reduction in risk, is difficult to measure. Thus, a reasonable interim step is to ask what capabilities have been enabled by the grant programs.

For the Port Security Grant Programs, the National Preparedness report begins to answer this question. Through this report, FEMA asks local jurisdictions to self-assess their preparedness across 31 core capabilities related to prevention, protection, mitigation, response, and recovery.<sup>10</sup> Focusing assessment of preparedness and security is a positive step in managing the grant programs. Yet performance measurement is still maturing. If we are to better answer the question of what port security or other grant programs have accomplished, evaluation must be improved in two ways.

---

<sup>9</sup> Victoria A. Greenfield, Valerie L. Williams, Elisa Eiseman (2006). *Using Logic Models for Strategic Planning and Evaluation*, TR-370-NCIPC, RAND Corporation, Santa Monica, CA.

<sup>10</sup> FEMA (2013). *National Preparedness Report*. Federal Emergency Management Agency, Washington, DC, March 30, 2013.

- First, subjective, self-reported evaluations can be supported by more reliable assessments – for example, using a system of audits and reviews or incorporation of functional drills and tests of component capabilities.
- Second, preparedness evaluation can assess whether communities have developed sustainable capabilities. Over time, capabilities can fade. Trained personnel retire or take new jobs. Equipment is consumed or becomes obsolete. Sustainability is not something that just happens, it must be planned for. Thus, preparedness and security assessments must describe whether security improvements can be expected to last.

For the issue of radiological detection, considerably less progress has been made in program evaluation. The Domestic Nuclear Detection Office (DNDO) is responsible for coordinating the government wide efforts to detect and interdict illicit trafficking of nuclear materials destined for the U.S. In 2011, the National Academy of Sciences concluded that DNDO was not able to make a compelling case for why advanced nuclear detection capabilities improved port security enough to justify the cost of acquiring and operating the equipment. At that time, the review panel, of which I was a member, recommended that DNDO improve the methods it uses to analyze the benefits of improved detection capabilities.<sup>11</sup>

In 2013, a second review panel of the National Academy of Sciences, of which I was not a member, made the same recommendation, concluding that over the two years between the assessments, little progress had been made.<sup>12</sup>

I urge Congress to continue to work with and support DHS to improve both our understanding of the current state of port security and the methods by which we assess it.

#### **Are the current priorities for port security grant programs correct?**

There is general consensus that priorities for the port security grant programs should be based on risk. Unfortunately, reliable methods for measuring risk at ports – especially terrorism risk at ports – remain elusive. Yet, greater reliance on local risk assessments in the award process could make ports more secure.

As currently managed, the port security grant program uses a two-stage process to allocate and award grants.<sup>13</sup> The first stage is commonly referred to as the risk assessment. At the risk assessment stage, DHS uses proxies of threat, vulnerability, and consequence to group ports into three tiers. The highest

<sup>11</sup> NAS (2011). *Evaluating the Testing, Costs, and Benefits of Advanced Spectroscopic Portals*. National Academy of Sciences, Washington, DC.

<sup>12</sup> NAS (2013). *Performance Metrics for the Global Nuclear Detection Architecture*. National Academy of Sciences, Washington, DC.

<sup>13</sup> For a more thorough description of the grant allocation process see GAO (2011). *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened*. GAO-12-47, Washington, DC.

Tier, Group 1, contains the ports judged to be at greatest risk. Groups 2 and 3 are judged to bear comparatively less risks. These groups define the amount of funding for which a port is eligible to compete.

In the second stage, the Award stage, project proposals are reviewed, ranked and selected. One input into this review is a risk assessment conducted at the port. This risk assessment considers which assets at the port may be at the greatest threat, may be most vulnerable to attack, and would lead to the most damage or destruction if attacked. The assessment also considers how the project would reduce vulnerabilities or consequences of an attack, and thus reduce risk.

Though imperfect, this process is a practical means for implementing risk-based allocation of grants. Though the first stage is referred to as a risk assessment, it is more aptly referred to as an assessment of importance of a port. For example, many of the proxies used reflect the size of the port or size of communities around the port. By using these measures, the "risk" score for the port security grant program is not changed by any of the funding applied to port security.

The second stage incorporates an assessment that is more appropriately referred to as a risk assessment. The port security risk assessments describe specific vulnerabilities and consequences at ports, which in theory change when proposed security countermeasures are implemented.

Greater reliance on local risk assessments and consultation with port security operators when awarding grant projects can improve how risk assessment is incorporated into setting priorities for port security.

**Should the 100% scanning requirement be implemented?**

Studies of this mandate demonstrate that there are ways it could be implemented, but raise questions about whether it should be.

DHS works with federal and international partners to detect and interdict illicit trafficking of nuclear materials or weapons. The system of cargo screening and scanning is designed around the premise that DHS can use shipping manifests along with knowledge of shippers, importers, and carriers to identify and focus inspections on shipments that pose the greatest threat of smuggling.

DHS concluded that this "risk-based" system, along with tips for smuggling investigations and some random inspections, provided the best balance of interdiction capability, deterrence, and minimal disruption of trade. As recently as 2012, the Secretary of DHS (then Janet Napolitano) decided not to implement the 100% container inspection requirement. Yet, the legislative mandate remains in effect.

In the years since the 100% requirement was enacted as law, it has been extensively studied. Analysis of port operations demonstrated that 100% scanning could be implemented at some of the world's largest ports.<sup>14</sup> However, assessment of the costs and benefits of this requirement raise questions about whether implementing 100% inspections is desirable:

- Do the benefits of 100% inspection justify the costs? Only for preventing nuclear detonations, but not dirty bombs and only if implementing the program doesn't cause shippers and carriers to modify their supply chains, adding costs and inefficiencies to freight transportation.<sup>15</sup>
- Would 100% inspection deter nuclear terrorism? Not significantly. While 100% inspection might dissuade nuclear smuggling via container shipping, would-be terrorists have many other ways to smuggle a nuclear weapon should they acquire one.<sup>16</sup>

If DHS is called upon again to explain whether or not the 100% container inspection will be implemented, I urge Congress to also consider at that time whether the mandate itself should be reconsidered.

Again, Chairman Carper, Ranking Member Coburn, and members of the Committee, thank you for inviting me to submit testimony on this very important issue for the nation.

---

<sup>14</sup> Nitin Bakshi, Stephen E. Flynn, and Noah Gans (2011). Estimating the Operational Impact of Container Inspections at International Ports. *Management Science*, Vol. 57, No. 1, pp. 1-20.

<sup>15</sup> See van de Voort, M., H. H. Willis, D. S. Ortiz, S. E. Martonosi (2007). Applying risk assessment to secure the containerized supply chain. In I. Linkov, R. J. Wenning, G. A. Kiker, *Managing Critical Infrastructure Risk*. Dordrecht, The Netherlands: Springer and Martonosi, S. E., D. S. Ortiz, H. H. Willis (2005). Evaluating the viability of 100 percent container inspections at America's ports. In H.W. Richardson, P. Gordon and J.E. Moore II, *The Economic Impacts of Terrorist Attacks*. Cheltenham, UK: Edward Elgar Publishing.

<sup>16</sup> Haphuriwat, N., V. Bier, H. H. Willis (2011). Deterring the Smuggling of Nuclear Weapons in Container Freight through Detection and Retaliation. *Decision Analysis* an INFORMS Journal, 8(2), 88-102.

**Post-Hearing Questions for the Record  
Submitted to Ms. Ellen McClain  
From Senator Tom Coburn**

**“Evaluating Port Security: Progress Made and Challenges Ahead”  
June 4, 2014**

<b>Question#:</b>	1
<b>Topic:</b>	PSGP
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Management of the grant program has consistently drawn criticism; FEMA has begun to eliminate the extended delay in the distribution of funds, which provides the grantees ample time to complete scheduled projects. Of all Port Security Grant Program (PSGP) funding awarded since FY07, only 43.7% has been expended (as of April 1st, 2013), this is a pattern that has been very consistent throughout the history of the program.

What steps have you taken to ensure the execution of all awarded funding?

**Response:** The Federal Emergency Management Agency (FEMA) recognizes that the Port Security Grant Program (PSGP) has had significant balances of unexpended dollars since FY 2007. FEMA has been proactive over the last several years to reverse this trend and has taken the following steps to achieve progress:

- FEMA is proactive in stakeholder outreach to encourage more frequent drawdowns.
- FEMA has changed the culture of granting no-cost performance period extensions by implementing a strict policy that sparingly extends awards based on established criteria, as outlined in FEMA GPD Information Bulletin No. 379, published February 17, 2012. All awards issued in fiscal years 2012 and 2013 have a two (2) year period of performance, encouraging grantees to prioritize spending their Federal dollars. FY 2014 awards will also carry a two (2) year period of performance.
- Beginning in FY 2009 and continuing through FY 2011 (while the Fiduciary Agent Model was in place), FEMA allowed grantees to align projects that closed gaps and vulnerabilities identified in local Area Maritime Security Plans (AMSPs) if their Port-Wide Risk Management Plans (PRMPs) were not already approved (a requirement that restricted

<b>Question#:</b>	1
<b>Topic:</b>	PSGP
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

the use of grant funding until the plan was approved). This allowed grantees to begin spending without waiting for the PRMP approval, thereby speeding up project implementation and drawdown.

- For those grantees utilizing funding for Transportation Worker Identification Credential (TWIC) compliance, FEMA has encouraged applicants to focus on installing TWIC infrastructure and purchasing readers that already have been tested by the Transportation Security Administration (TSA) and the U.S. Coast Guard (USCG) on an approved reader list that is published by TSA. Grantees also have the option of re-programming funding for other program priorities.
- FEMA developed a formal process to request cost-share waivers starting in FY 2009 and provided additional flexibility starting in FY 2012 to help speed the drawdown rate. A by-product of that process was an average 3-4 month delay while the request was approved. Over time the process has been refined and the average time required to process a cost share waiver currently is 4 weeks.
- The cost-share approval delegation now rests with the FEMA Assistant Administrator for Grant Programs. (Previously waivers were only approved by the Secretary of the Department of Homeland Security.)
- Beginning in FY 2013, FEMA required that applicants demonstrate an available cost share at the time of application or their application would not be considered for funding.
- Since FY 2012, the Port Security Grant Program (PSGP) has been a direct grant program whereby applicants apply directly to FEMA, and FEMA makes awards to those successful applicants without using a Fiduciary Agent (FA) as a pass-through entity. This has multiple benefits including the establishment of a direct relationship between FEMA and the grantee for grants management, which facilitates timely drawdowns and more detailed reporting.
- Over the last several years, FEMA has completed budget reviews prior to issuing awards, eliminating a hold on funding post-award, thereby giving grantees access to their funds more quickly. In addition, FEMA has eliminated holding funding pending Environmental and Historical Preservation (EHP) approval. The grantee still is responsible for compliance and is prohibited from beginning projects requiring an EHP review until that review is completed.

<b>Question#:</b>	1
<b>Topic:</b>	PSGP
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** What improvements in grant spending can be met by consolidating the Homeland Security Grant Programs into one National Preparedness Grant Program?

**Response:** The consolidation of grant programs (including the PSGP) under the National Preparedness Grant Program (NPGP) would provide several crucial benefits related to improved grant spending. First, consolidating the grant programs would allow state, local and private sector grantees (including ports) to collaboratively prioritize the investment of federal grant dollars to address the greatest needs. This would ensure that grant money is used effectively and efficiently to address security gaps and build capabilities. Strict enforcement of the two-year period of performance would ensure that grantees and subgrantees use grant dollars only for projects that can be completed within that timeframe, rather than spreading the money out over several fiscal years.

Second, State Administrative Agencies (SAAs) have extensive experience in managing many of FEMA's preparedness grant programs and have the staff and resources to effectively manage grants, thereby decreasing wait times for programmatic approvals and facilitating grant drawdowns. Finally, involving the SAA in the management of all preparedness grants flowing into a state would provide the state with the flexibility to re-allocate funding from entities that are not spending their money effectively to other entities that have needs and a demonstrated ability to execute projects in a timely manner.

<b>Question#:</b>	2
<b>Topic:</b>	deadline
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Secretary Napolitano notified Congress on May 3rd of 2012, that DHS was formally extending the July 2012 deadline by two years. Secretary Johnson made an identical notification to Congress on May 5th of 2014. The Chamber of commerce recently sent Sec. Johnson a letter representing 70 U.S. manufacturers, farmers, wholesalers, retailers, importers, distributors, and transportation and logistics providers fully supporting the recent decision to extend the deadline.

When will the Department meet the 100% scanning mandate?

**Response:** As noted by Secretary Johnson in his May 5<sup>th</sup> letter to Congress extending the July 2012 deadline for another two years, DHS is not able to meet the 2014 deadline (as extended by former Secretary Napolitano in 2012). Given the extensive operational, diplomatic, and fiscal challenges of the 100% scanning requirement, we cannot predict when DHS will meet the mandate.

**Question:** Do you expect DHS to extend this waiver in 2016? Is it an achievable goal, given the challenges noted in the June 4th hearing?

**Response:** If conditions remain constant, we expect the Department will exercise the waiver provision in the SAFE Port Act, as it has on two previous occasions. Achieving 100% scanning of U.S. bound maritime containers is not achievable in the foreseeable future unless new technology and other advances enable us to address the challenges of scanning transshipped cargo, enormous costs, impacts on global trade, and current port configurations. DHS assessments indicate that concentrating 100% of security assets on a single mode of transport will not reduce overall risk. Currently, DHS is improving port security with limited resources by using a risk based approach focused on high risk across all pathways.

<b>Question#:</b>	3
<b>Topic:</b>	DSIC
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Decision Sciences International Corporation (DSIC), an advanced technology provider of security and detection systems, was awarded a research and development contract by DHS' Domestic Nuclear Detection Office (DNDO) for an Advanced Technology Demonstration (ATD) of its Multi-Mode Passive Detection System (MMPDS) in 2012. The contract had an estimated value of \$2.7 million.

DNDO has evaluated Decision Sciences' Multi-Mode Passive Detection System technology; how far away is this technology actually working to accomplish improved scanning capability?

**Response:** DNDO initiated the Nuclear and Radiological Imaging Platform project in 2012 in an effort to characterize the ability of emerging technologies to detect radiological and nuclear materials, while clearing benign conveyances, regardless of shielding or cargo clutter levels. The project required that the selected developmental systems be able to detect 4 kilograms of highly enriched uranium. Initial tests in 2013 showed that DSIC's system did not meet this performance threshold. In June 2014, after additional development, DNDO conducted another milestone review. Although DSIC's system still does not meet the performance threshold, the system did demonstrate the ability to detect 8 kilograms of uranium in a controlled and limited environment (i.e., the factory) and is ready to begin an independent performance characterization in a controlled operational environment. This technology characterization is now scheduled to begin at Freeport Container Terminal in the Bahamas in Fall 2014. Subsequent data analysis will take approximately six to eight months with a final report following the analysis. The characterization includes an assessment of the technology readiness level, which will provide key information necessary to determine whether the technology is sufficiently mature for consideration in a DHS acquisition program. Data gathered by the Nuclear and Radiological Imaging Platform project will be used in DHS Analysis of Alternatives to identify whether any available technologies are suitable to meet DHS' needs.

**Question:** What is the total funding that has been appropriated for the testing of this type of technology testing by the Department (DNDO)?

**Response:** Since FY 2012, DNDO has obligated a total of \$18.0M to support the development and testing of solutions in the NRIP Project. An additional \$7.5M is included in the President's budget request for FY 2015 to complete the analysis and final report.

<b>Question#:</b>	3
<b>Topic:</b>	DSIC
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Other than Decision Sciences, how many other companies has DNDO worked or is working with on new scanning technology?

**Response:** Two other vendors were competitively awarded contracts for the Nuclear and Radiological Imaging Platform project. DNDO also is funding over ten basic and applied research projects that involve less mature technologies to address the challenge of detecting shielded nuclear material.

<b>Question#:</b>	4
<b>Topic:</b>	Acquisition Decision Memo
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** In an April 2013 document, “Acquisition Decision Memo,” assigned Action Item 1 to TSA & CG Senior Leadership to meet and identify opportunities for improving integration between organizations and to define TWIC roles and responsibilities.

Why is this being done 12 years after program creation years ago?

The findings and recommendations were to be presented in May 2013 meeting, what were those findings and recommendations?

**Response:** Since the inception of TWIC, TSA and USCG have worked together to administer the program. TSA is responsible for enrollment, security threat assessments, and systems operations and maintenance related to TWIC cards, while the USCG is responsible for the enforcement of regulations governing the use of TWIC cards at MTSA-regulated facilities and vessels. DHS directed TSA and USCG, at an Acquisition Review Board meeting on 28 March 2013, to define their respective TWIC programmatic roles and responsibilities and improve integration between the components. The roles and responsibilities were then presented, as directed by the Acquisition Decision Memo (ADM), to DHS leadership. Additionally, a TWIC Executive Steering Committee (ESC) was created, co-chaired by TSA and USCG, to provide effective governance, oversight, and guidance to the TWIC program and promote greater “unity of effort” for all related projects and initiatives. Close coordination between TSA and USCG, through the ESC, has been critical in reforming the TWIC enrollment and card issuance processes; providing greater awareness of the TWIC Reader Notice of Proposed Rulemaking; and improving a number of customer service concerns, such as implementing OneVisit, increasing call center capacity, creating web-based ordering for replacement cards, and enhancing quality assurance oversight of contractor performance at enrollment centers.

**Post-Hearing Questions for the Record  
Submitted to Ms. Ellen McClain  
From Chairman Thomas R. Carper**

**“Evaluating Port Security: Progress Made and Challenges Ahead”  
June 4, 2014**

<b>Question#:</b>	5
<b>Topic:</b>	scanning
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Thomas R. Carper
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** In his May 5, 2014, letter to Congress Secretary Johnson providing notification of his decision to renew the extension of the deadline for full-scale implementation of 100% scanning of U.S.-bound maritime cargo containers for an additional two years. In his letter, the Secretary stated that using currently available systems would lead to a negative impact on trade capacity and the flow of cargo. What progress has the Department made in researching and developing alternative technologies, including passive imaging systems that might be able to meet the statutory requirements?

**Response:** The 100% scanning of U.S.-bound maritime cargo containers requires scanning by “nonintrusive imaging equipment and radiation detection equipment” (6 U.S.C. §982 (b)(1)). The Department has conducted extensive research in technologies for nonintrusive imaging and radiation detection equipment, including basic research, applied research, and advanced technology demonstrations. An example of basic research is gravity gradiometer, a passive technique that uses gravity sensors to detect dense nuclear material and shielding material. Currently, the Nuclear and Radiological Imaging Platform advanced technology demonstration is developing and assessing passive and active techniques to detect shielded threats. Advanced technology demonstrations culminate in a technology characterization, including an assessment of the technology readiness level, which will provide key information necessary to determine whether technology is sufficiently mature for consideration in DHS acquisition programs.

To date, technologies capable of imaging and radiation detection while meeting the technical scanning equipment requirements of the law do not address the challenges and adverse impacts to the trade caused by the delays in adjudicating alarms, the inability to scan transshipped containers without unloading, and foreign partners’ reluctance to permit the installation of these systems.

**Post-Hearing Questions for the Record  
Submitted to RDML Paul Thomas  
From Senator Tom Coburn**

**“Evaluating Port Security: Progress Made and Challenges Ahead”  
June 4, 2014**

<b>Question#:</b>	1
<b>Topic:</b>	MSRAM
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** During the June 4th hearing, you made a statement about the Coast Guard’s Maritime Security Risk Analysis Model (MSRAM) being utilized annually by FEMA in the process to determine Port Security Grant Program’s Group Tiering. Can you provide all uses of the MSRAM for the Port Security Grant Program?

**Response:** The Coast Guard’s Maritime Security Risk Analysis Model (MSRAM) supports the Port Security Grant Program (PSGP) in two ways. First, MSRAM provides data for the National Infrastructure Index of the grant program’s risk formula which is incorporated into FEMA’s “Group-Tiering.” This includes consideration for risk bought down from previous grant rounds. Second, MSRAM data is used to assist FEMA in their analysis of individual grant applications.

<b>Question#:</b>	2
<b>Topic:</b>	TWIC 1
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The TWIC program is in its 12th year, more than \$453 million (according to most non-governmental sources) has been spent on the program and TSA has issued over 2.4 million active cards, yet program implementation is not yet complete. Why is this program not completed? What are the challenges that have delayed this complete implementation?

**Response:** The Maritime Transportation Security Act (MTSA) of 2002 directed the Department of Homeland Security to issue regulations to require credentialed merchant mariners and transportation workers seeking unescorted access to secure areas of MTSA-regulated facilities, vessels, and Outer Continental Shelf facilities undergo a security threat assessment and receive a Transportation Worker Identification Credential (TWIC).

Since that time, TSA and the USCG have jointly implemented the TWIC Program at thousands of MTSA regulated facilities and vessels and issued more than 2.9 million TWICs to transportation workers nationwide. The agencies have also conducted extensive outreach with the public, industry and other stakeholders involved, issued numerous policies and guidance documents to assist in the implementation and enforcement of the TWIC Program, and released the TWIC Reader Notice of Proposed Rulemaking. We expect to release the TWIC Reader Rule in 2015. Since releasing the NPRM in March 2013, the USCG has addressed over a thousand unique questions and comments provided by more than 150 commenters during the NPRM public comment period in preparation of the final rule.

Through the initial rulemaking process, conducted in 2006, the Department of Homeland Security (DHS) concluded that facility and vessel operators would not be required to purchase or install electronic TWIC readers during the initial issuance of TWIC cards. Meanwhile, the vetting of persons seeking access to the secure areas of regulated vessels and facilities provided a tremendous advance in security, even without the immediate implementation of a reader requirement.

The Security and Accountability For Every Port Act of 2006 (SAFE Port Act) (P.L. 109-347) then directed DHS to conduct a TWIC Reader Pilot Program (Reader Pilot) to inform a second rulemaking that would focus specifically on the use of the TWIC cards with biometric readers. DHS could not begin the TWIC Reader Pilot Program until after April 15, 2009, when the requirement for MTSA facilities to implement TWIC as an access control tool using visual examination of the card and verification of the individual's purpose for seeking access became effective.

DHS completed the TWIC Pilot Program in the summer of 2011 and published the Pilot Report in February of 2012. The Coast Guard then published the NPRM in March of 2013. To develop the NPRM, the Coast Guard reviewed the results of the Pilot Program

<b>Question#:</b>	2
<b>Topic:</b>	TWIC 1
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

and worked with TSA, evaluating complex biometric reader technologies and assessing equipment performance and reliability. The Coast Guard also evaluated how the final TWIC Reader Rule would impact businesses' training requirements, changes and upgrades to infrastructure, environmental obstacles, user interface and impact on throughput times, and other factors. The Coast Guard is now reviewing the suggestions the public provided during the 90 day public comment period to refine and improve the rule. We are now working to release the TWIC Reader Final Rule as quickly as possible.

**Question:** When will the program be completely implemented?

**Response:** Public comments received from the TWIC Reader NPRM are under review as the Coast Guard prepares to release the TWIC Reader Final Rule. In the NPRM, Coast Guard proposed a 2-year implementation phase for MTSA facilities to come into compliance with the new regulations.

<b>Question#:</b>	3
<b>Topic:</b>	NPRM
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Coast Guard recently issued a Notice of Proposed Rulemaking (NPRM). The Port Industry has provided vehement opposition to the recent NPRM, due to the failure to utilize a risk-based approach to reader requirements that adequately addresses the particular circumstances of each port area and the facilities that fall within the category requiring readers. What has been your response to the American Association of Port Authorities and the National Association of Waterfront Employers?

**Response:** The Coast Guard received over 100 submissions expressing over 1,200 unique comments, questions, and concerns. Many of the comments expressed strong support for the NPRM, others provided narrowly focused suggestions, while some were more critical. Regardless, the Coast Guard carefully reviewed all of the comments and we will use them to inform and improve the final rule.

The Coast Guard used risk analysis to assess the risk of an incident involving regulated vessels and facilities rising to the level of a Transportation Security Incident (TSI) as defined in the Maritime Transportation Security Act of 2002, for scenarios for which TWIC and TWIC Readers provide risk mitigation. The Coast Guard believes the existing risk analysis model described in greater detail in the TWIC Reader Notice of Proposed Rulemaking, and which considered a wide range of targets, attacks, and consequences, remains the most comprehensive and logical means available to implement the electronic TWIC inspection program.

<b>Question#:</b>	4
<b>Topic:</b>	MTSA
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Under MTSA, the Coast Guard regulates approximately 13,825 vessels, 3,270 facilities, and 56 Outer Continental Shelf (OCS) facilities. Of those MTSA-regulated facilities that could have potentially been regulated, only 38 vessels (0.27%) and 532 facilities (16%) are affected by this proposed rule. With less than 20% of facilities and less than 1% of vessels being required to have biometric card readers based on the new rule; how has this decision improved the security at the remaining facilities and vessels?

**Response:** The Coast Guard's analysis indicates that relative to their costs, electronic readers would provide only limited security benefits to certain MTSA-regulated facilities and vessels at this time. The proposed rule balances the need for better security where risk is greatest, without imposing undue burdens where risk is lower. Note that these facilities and vessels are still required to use TWIC as part of their access control measures, including a requirement to visually assess certain security features in the TWIC.

Whether used with visual inspection or an electronic reader, TWIC is one element within a layered approach to port security. All TWIC holders receive a security threat assessment (STA) that includes checks for ties to terrorism, criminal history, and lawful status. A properly vetted workforce maintains the safety, security, and integrity of our nation's ports.

TWIC is only the first half of a two-part process. First, vessel and facility security personnel must determine that an individual possesses a valid TWIC. Second, they must assess the individual's business case for entering a vessel or facility before granting the individual unescorted access. The TWIC provides a means by which a vessel or facility security officer can determine that an individual has been properly vetted. 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/vessels based on the valid TWIC and business case.

TWIC is nationally recognized. 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.

<b>Question#:</b>	4
<b>Topic:</b>	MTSA
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** How does this impact the other 13,787 vessels and 2,738 facilities that have been under the assumption for the past 12 years that they would be required to have the card readers?

**Response:** MTSA-regulated facilities and vessels exempt from using readers under the proposed rule, based upon assessed risk, would continue to comply with the TWIC program as required in 33 CFR Parts 101, 104, 105, and 106.

<b>Question#:</b>	5
<b>Topic:</b>	TWIC 2
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Coast Guard has admitted that greater security benefits are obtained when a biometric verification is conducted at each required presentation of the TWIC through the use of an approved TWIC reader. This is the only way to ensure that the individual presenting the TWIC is in fact the individual whose background and criminal history was vetted by TSA and that the TWIC presented has not been revoked by the TSA. Why was the decision made contrary to the March 2009 recommendation in the Advanced Notice of Proposed Rulemaking, which would require Risk Groups A & B to have card readers?

**Response:** The Coast Guard performed extensive risk analyses to assess the effectiveness potential risk reduction of requirements for TWIC readers in preventing or mitigating a Transportation Security Incident (TSI), as defined in the Maritime Transportation Security Act of 2002 (MTSA). The Coast Guard used the risk analysis model described in the TWIC Reader Notice of Proposed Rulemaking, which considered a wide range of targets, attacks, and consequences, to determine where TWIC readers are deployed. This assessment showed a clear delineation in the risk to Risk Group A facilities versus all other facilities.

The Coast Guard used risk analysis to assess the risk of an incident involving regulated vessels and facilities rising to the level of a Transportation Security Incident (TSI) as defined in the Maritime Transportation Security Act of 2002, for scenarios for which TWIC and TWIC Readers provides risk mitigation. The Coast Guard believes the existing risk analysis model described in greater detail in the TWIC Reader Notice of Proposed Rulemaking, and which considered a wide range of targets, attacks, and consequences, remains the most comprehensive and logical means available to implement the electronic TWIC inspection program.

Additionally, after performing a thorough cost-benefit analysis, Coast Guard concluded that the benefit of TWIC readers at Risk Group A facilities and vessels justifies the cost of deployment. Risk Group A contains 5 percent of the MTSA-regulated population, which represents approximately 80 percent of the potential consequences of a Transportation Security Incident (TSI). The NPRM evaluated other combinations of potential affected populations, but all provided limited risk reduction potential in comparison to the costs. However, vessels and facilities identified in any risk group are free to use readers on a voluntary basis.

In accordance with MTSA and the SAFE Port Act, the Coast Guard conducts annual exams as well as announced and unannounced spot checks to verify facilities are operating in accordance with approved Facility Security Plans (FSP). A component of these Coast Guard exams is inspecting the access control provisions and the implementation of the TWIC. These exams and spot checks happen today and include the use of mobile

<b>Question#:</b>	5
<b>Topic:</b>	TWIC 2
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

biometric readers to verify the identity of TWIC holders. These enforcement activities would continue, and potentially increase, for all risk groups under the proposed rule. The Coast Guard will continue to evaluate the requirements imposed on all risk groups and, if our analyses justify the need for further deployment of readers, we may propose additional requirements.

**Question:** Please explain the option for vessels and facilities to move between Risk Groups based on cargo handled?

**Response:** Many regulated vessels and facilities retain the flexibility to change and evolve operations depending on a variety of factors. Market demands, environmental impacts, and operational capabilities are a few of the factors that may influence how and in what capacity a vessel or facility will operate. Hence there is the possibility that a vessel/facility may change its operations that will cause it to fluctuate between needing to implement the use of TWIC readers and not needing to implement TWIC readers. If a vessel or facility finds that their operations are no longer “high risk” as specified in the proposed regulation, they may drop from Risk Group A and be eligible to dispense with the need for TWIC readers.

Specifically, in the NPRM, the Coast Guard stated that it proposed adding §§ 104.263(d) and 105.253(d) to “address the movement between risk groups by vessels and facilities, based on the materials they are carrying or handling, or the types of vessels they are receiving at any given time.” These provisions would provide flexibility to owners and operators of vessels and facilities that only meet the criteria for Risk Group A classification on an infrequent or periodic basis, such as a facility that only occasionally receives a shipment of bulk Certain Dangerous Cargo (CDC).

<b>Question#:</b>	6
<b>Topic:</b>	TWIC 3
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Coast Guard is responsible for assessing and enforcing operator compliance with TWIC-related laws and regulations. Can you explain your role in TWIC?

**Response:** Coast Guard field units are responsible for:

- Ensuring MTSA regulated facilities and vessels are in compliance with TWIC provisions;
- Conducting TWIC validation and authentication checks during annual compliance exams and security spot checks on regulated facilities and vessels;
- Reviewing and approving amendments to Facility Security Plans (FSPs) and Vessel Security Plans (VSPs); and
- Identifying alleged, suspected, or actual incidents of forged or counterfeit TWIC cards and appropriately referring cases to Coast Guard Investigative Service (CGIS) for criminal investigation.

**Question:** How do you currently enforce compliance of the program?

**Response:** In accordance with MTSA and the SAFE Port Act, the Coast Guard conducts annual exams as well as announced and unannounced spot checks to verify facilities are operating in accordance with approved Facility Security Plans (FSP). A component of these Coast Guard exams is inspecting the access control provisions and the implementation of the TWIC.

**Question:** How will that change once the biometric card readers have been implemented?

**Response:** The Coast Guard will enforce TWIC Reader requirements using the policies and procedures currently in place for enforcing existing MTSA regulatory requirements for vessels and facilities in Risk Group A. Inspectors will confirm that applicable vessels and facilities use readers for access control in accordance with their approved security plans. Non-Risk Group A facilities or vessels that choose to voluntarily operate with TWIC readers must document their use in the approved security plan and are expected to be in compliance with their own stated security measures. Furthermore, the MTSA regulations contain existing provisions in 33 CFR 104.235, 104.260, 105.225, 105.250, 106.230, and 106.255 require that all security systems, equipment, and TWIC readers are maintained in proper working order.

<b>Question#:</b>	7
<b>Topic:</b>	International Port Security Program
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Will you detail the mission of the International Port Security Program and articulate its need for cooperation and coordination in the maritime domain?

**Response:** As directed by the MTSA, the International Port Security (IPS) Program periodically assesses the effectiveness of anti-terrorism measures in the ports of nations conducting maritime trade with the United States (approximately 150). If the Coast Guard does not find that effective anti-terrorism measures are in place as a result of that assessment, Conditions of Entry are placed on vessels arriving to the United States from those ports and those vessels are required to implement additional security measures. The IPS Program cannot compel countries to allow its teams to visit their country to conduct the assessment; therefore, the Coast Guard attempts to utilize a cooperative approach by conducting capacity building to help countries improve their security, and offering reciprocal visits, i.e. allowing representatives of U.S. trading partners to visit the U.S. to observe how the Coast Guard manages port security.

**Question:** What kind of information is gained by assessing the potential threat foreign ports pose to the maritime supply chain?

**Response:** The Coast Guard gains situational awareness of the level of the implementation of an international security standard, the International Ship and Port Facility Security (ISPS) Code in the trading partners of the U.S. The Coast Guard is able to make an informed decision regarding the potential risk of a terrorist or weapon of mass destruction being able to be surreptitiously introduced onto a vessel and then transferred to the homeland. Vessels arriving to the U.S. from facilities found to have ineffective anti-terrorism measures in place primarily due to the fact that the facilities are not ISPS Code compliant pose a higher risk to the U.S.

**Post-Hearing Questions for the Record  
Submitted to Mr. Kevin K. McAleenan  
From Senator Tom Coburn**

**“Evaluating Port Security: Progress Made and Challenges Ahead”  
June 4, 2014**

<b>Question#:</b>	1
<b>Topic:</b>	cargo security
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** DHS utilizes a multi-layered approach to cargo security, including enhanced screening requirements for known and established shippers, explosive detection canine teams, and covert tests and no-notice inspections of cargo operations. On average, only about 2%-4% of all cargo containers are scanned.

Can you explain the strategy of CBP's C-TPAT, ATS and CSI programs?

**Response:** The decentralized nature of today's threat demands that we continue to move away from one-size-fits-all security approaches and toward risk-informed, intelligence-driven approaches. U.S. Customs and Border Protection's (CBP) layered and risk-based approach provides that, at a minimum, 100 percent of high risk cargo is examined through a number of measures, including screening, scanning, physical inspection, or resolution by foreign authorities. In addition, CBP has strengthened its Automated Targeting Systems (ATS) and enhanced the quality and timeliness of the commercial data upon which those systems rely. Security risks are further reduced by leveraging programs such as the Container Security Initiative (CSI) for the integrated scanning of high-risk cargo, the Customs-Trade Partnership Against Terrorism (C-TPAT) to foster security in member supply chains, and the Importer Security Filing (often called "10+2") for the advance collection of manifest and import data to enhance targeting.

ATS is a critical decision support tool that is the cornerstone for all CBP targeting efforts. CBP uses ATS to improve the collection, use, analysis, and dissemination of intelligence to target, identify, and prevent potential terrorists and terrorist weapons from entering the United States, and identify other violations and violators of U.S. law. In this way, ATS allows CBP Officers to focus their efforts on travelers and cargo shipments that most warrant further attention. ATS standardizes names, addresses, conveyance names, and similar data so these data elements can be associated with other business data to form a more complete picture of a traveler, import, or export in context with previous behavior of the parties involved. Every traveler and all shipments are processed through ATS and

<b>Question#:</b>	1
<b>Topic:</b>	cargo security
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

are subject to a real-time, rule-based evaluation. Risk assessment strategies are multi-tiered in their approach and are founded on complex statistical studies, data analysis, and rules based on knowledge engineering. On a typical day, CBP, using ATS, conducts 100 percent risk assessments on the nearly one million travelers and over 66,000 containers entering at our air, land, and sea ports of entry.

As a key component of CBP's layered cargo enforcement strategy, the C-TPAT partnership program establishes clear supply chain security criteria for members to meet and in return provides incentives and benefits like expedited processing. C-TPAT continues to apply tangible trade facilitation to C-TPAT Partners in light of their demonstrated commitment to adopt stronger security practices throughout their international supply chains. In a 2010 C-TPAT Cost and Savings Survey (available on the CBP website), respondents noted that the value of C-TPAT membership goes beyond dollars and cents; it includes risk avoidance, a communal approach to a safer supply chain, being able to compete for contracts that require C-TPAT membership, and taking advantage of the credibility that C-TPAT membership brings.

CSI was announced in January 2002 to protect the United States from terrorism and acts of terror in the international maritime supply chain while facilitating legitimate trade. As part of CSI, CBP officers are stationed in foreign seaports to work together with host government counterparts to share information, develop additional investigative leads on terrorist threats related to cargo destined for the United States and identify potential high-risk shipments. Cargo identified as high-risk is examined using a variety of risk mitigation tactics, including large scale x-ray imaging equipment and radiation detection equipment.

**Question:** How confident are you that these programs provide adequate security for the cargo containers that enter U.S. ports?

**Response:** C-TPAT Partners are required to notify C-TPAT of any major changes that affect their overall operations and security of their supply chains. These changes may include an importer sourcing from a new country; major acquisitions; and heightened security threats in countries of an importer's supply chain. C-TPAT Specialists are required to vet all of their companies on a yearly basis to ensure that all Partners are still eligible to participate in the program. This annual vetting requirement ensures that C-TPAT Partners have not been subject to a security incident that the Partner may have failed to report to CBP as required by the program.

Approximately 80 percent of all maritime containerized cargo destined to the United States originates in or transits through a CSI port. CBP Officers stationed in those ports

<b>Question#:</b>	1
<b>Topic:</b>	cargo security
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

review 100 percent of all the bills of lading and those shipments identified as high risk are examined prior to lading on the vessel; this accounts for 85 percent of all high risk shipments destined for the United States. In Fiscal Year 2013, 99 percent of all examination requests were conducted in the foreign CSI ports.

CSI, along with other CBP and U.S. Government security programs, combine to secure the global supply chain while expediting the movement of legitimate cargo. CBP is confident that these cargo security programs provide a good balance between facilitating the movement of legitimate cargo while continuing to secure the homeland and continues to refine and improve our systems and cargo security programs to better serve these priorities.

**Question:** How much more secure would scanning 100% of all containers make U.S. ports?

**Response:** A recent study by Domestic Nuclear Detection Office suggested that concentrating all resources and efforts on a single pathway, maritime containerized cargo, would have little effect on overall security. Consequently, we balance our efforts across pathways commensurate with the risk that each one poses, and utilize programs such as CSI and C-TPAT and tools such as ATS, TECS, Automated Commercial Environment, open source information, and intelligence provided by our foreign counterparts, in order to identify potentially high risk cargo and mitigate the threat posed by such cargo. In CSI locations, all cargo is screened for such threats and 100 percent of all cargo deemed high risk is examined. Additional CBP initiatives such as C-TPAT and Trusted Trader further mitigate the threat posed by maritime cargo through the processes implemented by these programs.

**Question:** Does the technology exists that would allow DHS to meet the 100% scanning mandate?

**Response:** Technology does not currently exist that can effectively and efficiently scan the enormous amount of cargo required under the mandate, particularly transshipped cargo. Technology is only one part of the many challenges associated with the implementation of the mandate.

<b>Question#:</b>	2
<b>Topic:</b>	secure freight
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Due to challenges identified during the Secure Freight Initiative's pilot program, all operations, with the exception of Port Qasim, Pakistan, have reverted from the 100 percent scanning model to the risk based targeting approach of the Container Security Initiative program to optimize results through advanced analysis of manifest data and identification of high-risk cargo.

What diplomatic, technological, and operational challenges have clearly illustrated that current scanning technology adversely impacts trade capacity and the flow of cargo?

**Response:** The challenges implementing 100% scanning are numerous and significant. In terms of logistical challenges, many ports do not have a single chokepoint through which all the cargo passes. Instead, cargo moves through the port and onto vessels along multiple pathways, each of which would require deployment of large-scale scanning equipment. Moreover, in many locations, cargo is "transshipped," meaning it is moved immediately from vessel to vessel within the port. To be scanned, transshipped cargo must be offloaded, funneled through scanning equipment, and reloaded aboard the vessels. Most ports are not configured to put in place detection equipment or to provide space for secondary inspections. Scanning 100 percent of cargo with current systems is currently unworkable at many ports without seriously hindering the flow of shipments or redesigning the ports themselves, which would require huge capital investments and protracted negotiations with the foreign governments responsible for the approximately 800 ports worldwide that ship goods to the United States.

Other challenges to full implementation of the 100 percent scanning mandate relate to the limitations of available technology. CBP currently uses both passive radiation detection and active x-ray scanning to look for radioactive material in cargo at ports of entry both in the United States and abroad. A significant obstacle is the absence of an automated x-ray scanning technology that can effectively detect suspicious anomalies within cargo containers and trigger additional inspection. Currently, CBP personnel visually inspect screens for possible anomalies, but the scale and the variety of container cargo make this process resource intensive and impractical when applied to 100 percent of the approximately 12 million containers that enter the United States each year.

In addition, 100 percent scanning is difficult to achieve diplomatically, as it requires a burdensome, unfunded mandate on our international partners, Customs administrations, border security forces, port operators, and other entities. The cost of compliance for 100 percent scanning is extraordinary for these entities, for which they will receive little

<b>Question#:</b>	2
<b>Topic:</b>	secure freight
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

added value. CBP has found greater success in forming partnerships with these entities, via pilot programs, bi-lateral and multi-lateral information sharing, sharing of best practices, capacity building, and other activities. The growth of collaboration and mutual assistance, and the implementation of risk-based assessments have done far more to further better port and international supply-chain security at significantly less cost than the proposed 100 percent scanning requirement. Lastly, 100 percent scanning is perceived by our international partners as benefiting only the United States, while the aforementioned activities benefit the entire supply chain. Allowing CBP to prevent, detect, and investigate threats through nuanced searches and analysis and information sharing will tax our resources (domestically and internationally), while also negatively affecting our relationship with our trading partners, for too little gain.

**Question:** Can systems to scan containers be purchased, deployed, or operated at all ports overseas?

**Response:** The technology does not currently exist to efficiently and effectively scan all cargo at sea ports overseas. If the technology did exist, it would have to be built, configured, purchased, and deployed to the approximately 800 overseas ports which ship goods to the United States; this process would take years to accomplish. There is also the issue of which country or entity would pay for this acquisition, installation, operation, and maintenance. Operation of the scanning equipment requires personnel that have the authority and training to operate the machinery, read the scan data and mitigate any anomaly. This would require deploying personnel from the U.S. Customs and Border Protection or specially trained personnel in a foreign country. In some countries this may involve several different agencies and would require several different agreements.

**Question:** What are the physical characteristics required to install such a system?

**Response:** Many ports do not have a single checkpoint through which all the cargo passes. Instead, cargo moves through the port and onto vessels along multiple pathways, each of which would require deployment of large-scale scanning equipment. Moreover, in many locations, cargo is "transshipped," meaning it is moved immediately from vessel to vessel within the port. To be scanned, transshipped cargo must be offloaded, funneled through scanning equipment, and reloaded aboard the vessels.

Most ports are not configured to put in place detection equipment or to provide space for secondary inspections. Scanning 100 percent of cargo with current systems is currently unworkable at many ports without seriously hindering the flow of shipments or redesigning the ports themselves. The systems require a significant "footprint" for

<b>Question#:</b>	2
<b>Topic:</b>	secure freight
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

installation and most ports do not have the additional land to devote to installing multiple systems in a port.

<b>Question#:</b>	3
<b>Topic:</b>	DOD Inspector General report
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** A recent DOD Inspector General report revealed that 52 convicted felons received routine, unauthorized installation access, placing military personnel, dependents, civilians, and installations at an increased security risk. It was determined that this lapse occurred because the Navy Installations Command did not perform a comprehensive business case analysis and issued policy that prevented transparent cost accounting of Navy Commercial Access Control System.

What actions have been done taken to correct this security threat from happening in the future?

**Response:** The question is best answered by the Department of Defense.

**Post-Hearing Questions for the Record  
Submitted to Mr. Kevin K. McAleenan  
From Senator Thomas R. Carper**

**“Evaluating Port Security: Progress Made and Challenges Ahead”  
June 4, 2014**

<b>Question#:</b>	4
<b>Topic:</b>	GAO report
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Thomas R. Carper
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** According to a recent report by the GAO on the 2013 Sequestration (GAO-14-452, May 2014, page 21), CBP Office of Field Operations cited effects on cargo operations resulting from sequestration. What was effect of the sequester and the ongoing shortage of CBP Officer and Agriculture Specialist staffing on commercial vessel cargo and crew inspection and clearance at seaports?

**Response:** Due to sequestration, U.S. Customs and Border Protection’s (CBP) Office of Field Operations (OFO) was forced to reduce overtime expenditures at ports of entry around the country. OFO uses overtime to enhance coverage and primary staffing during peak periods and to perform enforcement actions at air, land, and sea ports of entry.

At our seaports, OFO did notice delays in the release of commercial vessel cargo due to the displacement of CBP Officers to the airport environment to minimize air passenger wait times. However, CBP worked to prioritize examinations based on threats and to address agricultural holds on perishables in a timely manner to minimize disruptions in trade. The majority of the inspections performed by CBP Officers and Agriculture Specialists were conducted during normal working hours. In some instances, cargo that was typically inspected by Agriculture Specialists and/or CBP Officers on overtime was therefore delayed 2-3 days, until such time the officers could get to the backlog during normal working hours. Significant delays in the release of commercial cargo were reported at Long Beach, California; Miami, Florida; and Port Everglades, Florida.

In addition, Long Beach and Port Everglades also reported increased processing times of 6.5 hours to process passengers and crew members on cruise ships due to the reduction in CBP Officers. Normal processing times for cruise ships is approximately 4 hours.

<b>Question#:</b>	5
<b>Topic:</b>	new CBP officers
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Thomas R. Carper
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Congress appropriated funds in fiscal year 2015 for 2000 new CBP officers. How many of the 2000 new CBP officers will be devoted to seaports? How are you evaluating projected increases in trade and cruise volumes and how any additional officers will be allocated to different ports of entry?

**Response:** U.S. Customs and Border Protection's (CBP) workload staffing model is used to assess the number of officers needed for each facility. It is based on volume, the number of examinations and other activities and duties CBP Officers perform on a daily basis, and the time required completing them. Overall 44 ports of entry in 18 states will receive additional staffing that will reduce wait times and help facilitate legitimate trade and travel. Although CBP does not release the allocation plan in its entirety due to security concerns, CBP considered operational factors such as service levels, enforcement, and future growth when identifying those ports in need of additional staff. Ultimately, most ports of entry continue to have staffing needs and CBP endeavors to better meet those needs with additional staff through a strategy outlined in the Fiscal Year 2015 President's Budget.

CBP works with importers and the shipping industry, as well as paying attention to trade growth estimates from the World Trade Organization and others. For cruise estimates, we work directly with the cruise line industry.

<b>Question#:</b>	6
<b>Topic:</b>	radiation screening
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Thomas R. Carper
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** What steps has CBP taken to facilitate radiation screening at seaports with on-dock rail facilities?

**Response:** In 2009, to comply with the *Security and Accountability For Every Port Act of 2006*, U.S. Customs and Border Protection (CBP) began scanning all rail-bound containers (commonly called “on-dock rail”) using mobile Radiation Portal Monitors (mRPM) at seaports that exclusively use straddle carriers for container movements. This concept of operation (CONOP) is employed within the top 22 seaports by volume. While effective in scanning containers, the CONOP is inefficient. The CONOP requires the terminal owner/operator to remove each container from the vessel into a holding area. Multiple containers are then moved from the holding area and stacked in a single row. A CBP Officer then drives the mRPM down one side and up the opposite side of the row of containers while the mRPM scans for illicit radiological and nuclear isotopes. Once the entire row is scanned, the terminal owner/operator then has to move the containers to the rail yard. This requires the terminal operator/owner to perform an extra container movement and set-aside significant real estate to facilitate the CONOP. The CONOP requires multiple CBP personnel and dedicated mRPM assets.

A new approach is being developed at the TraPac terminal in the Port of Los Angeles, California. The strategy is to automate its container handling and transportation system through the use of driverless straddle carriers with straddle carrier-mounted scanning system for rail-bound containers. The “new” radiation scanning technology will consist of existing operationally deployed Science Applications International Corporation/Leidos fixed Radiation Portal Monitor 8 (RPM8) systems integrated with a conveyor system. Automated straddle-carriers will convey ship-to-rail Intermodal Cargo Container to the conveyor-Radiation Portal Monitor system for radiation scanning.

**Post-Hearing Questions for the Record  
Submitted to Mr. Kevin K. McAleenan  
From Senator Thomas R. Carper**

**“Evaluating Port Security: Progress Made and Challenges Ahead”  
June 4, 2014**

<b>Question#:</b>	7
<b>Topic:</b>	Clearing International Passengers
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Carl Levin
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Procedures for Clearing International Passengers Arriving at U.S. Ferry Terminals International cruise ships dock at the Detroit/Wayne County Port Authority Public Dock and Terminal which has the capacity to accommodate vessels with as many as 400 passengers. Port Authority officials would like to be able to clear the passengers into the United States in the most efficient and convenient manner. That is accomplished inside its terminal as Customs and Border Protection (CBP) officials have done in the past on occasion using CBP laptop computers. However, at other times CBP officials have cleared passengers with CBP laptop computers from outside the building, or on the vessel, neither of which is as efficient as clearing passengers inside the building using those same laptop computers.

There is concern that if passengers cannot be cleared in the more efficient way from inside the terminal building the cruise ships will dock in Windsor instead of Detroit.

If the cost of installing CBP approved permanent equipment in the terminal is prohibitive, can the CBP at least on a regular basis use the most efficient means available to clear international passengers, which is inside the terminal building using CBP laptop computers?

**Response:** The Federal Inspection Station (FIS) at the Detroit Public Dock facility remains unfinished. It lacks required information technology infrastructure and equipment, and does not meet U.S. Customs and Border Protection’s (CBP) minimum security requirements. CBP Detroit will not be able to process passengers in the FIS until the facility is compliant with CBP requirements. In the interim while the Port Authority continues to seek the funding necessary to complete the FIS, CBP has remained flexible, working with the Port Authority to accommodate cruise ships that call in Detroit. Passengers disembark and are processed pier-side, or in the event of inclement weather, a common area on the vessel may be utilized for passenger processing. CBP Detroit remains committed to processing cruise ships that are scheduled to call in Detroit, but

<b>Question#:</b>	7
<b>Topic:</b>	Clearing International Passengers
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Carl Levin
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

will not process passengers in the FIS at the Detroit Public Dock until construction is completed in compliance with CBP requirements.

**Post-Hearing Questions for the Record  
Submitted to Mr. Brian Kamoie  
From Senator Tom A. Coburn, M.D.**

**“Evaluating Port Security: Progress Made and Challenges Ahead”**

**June 4, 2014**

<b>Question#:</b>	1
<b>Topic:</b>	PSGP 1
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Department of Homeland Security has spent \$2.9 billion in port security upgrades and equipment, Federal Emergency Management Agency (which oversees the program) currently has no method to determine whether any investment has improved the safety and security of our nation’s ports or measurably reduced the risk of a potential terrorist attack. Why has FEMA not developed performance metrics for the PSGP? How does FEMA determine port security improvements in the PSGP?

**Response:** The Federal Emergency Management Agency (FEMA) has made progress in assessing grant effectiveness under the National Preparedness Goal and National Preparedness System, which established measurable goals and objectives that enable FEMA to systematically evaluate changes in state-wide preparedness.

For the Port Security Grant Program (PSGP), FEMA works with the United States Coast Guard (USCG) and port security stakeholders to develop and implement frameworks that enable assessment of grant award allocation against maritime risks, which vary from port to port. The PSGP uses a comprehensive risk methodology to determine program grouping and grant funding allocations each year. This risk methodology captures threat, vulnerability, and consequence data for each eligible port entity, derived from subject matter experts in the Department of Homeland Security (DHS) as well as from publicly available data sources. This risk analysis provides DHS with an in-depth picture of each eligible port area’s risk landscape, which informs how FEMA prioritizes grant funding to address the highest risks facing the port.

Additionally, FEMA relies on the expertise of each port’s Area Maritime Security Committee (AMSC), which is comprised of stakeholders from private organizations, local law enforcement and first responders, and other locally-based Federal representatives, to identify gaps or vulnerabilities in port security. Through their Area Maritime Security Plans and assessments, AMSCs help ensure grant funding is applied to address the areas of greatest need, including the prevention of, detection of, response to, mitigation of, and/or recovery from attacks involving improvised explosive devices and

<b>Question#:</b>	1
<b>Topic:</b>	PSGP 1
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

other non-conventional weapons. In his or her role as Federal Maritime Security Coordinator, the USCG Captain of the Port also reviews projects submitted for grant award in order to verify and prioritize how they address port security gaps and vulnerabilities, including those identified in industry-created Facility and Vessel Security Plans. Completion of PSGP projects reduces identified port security gaps and vulnerabilities.

A Federal level review by FEMA and the USCG validates each port's priorities and ensures that grant awardees are addressing National program priorities, which helps to achieve the goal of a secure and resilient nation. Projects funded through PSGP play an important role in improving the ability to deliver core capabilities and also in the maintenance and sustainment of core capabilities. PSGP funding specifically supports the implementation of risk mitigation strategies as outlined in Area Maritime Security Plans which address security gaps and vulnerabilities identified in USCG Area Maritime Security Assessments. FEMA has developed specific measures to track the building and sustainment of capabilities with PSGP funding. FEMA began collecting data in fiscal year (FY) 2013 for the measures, "Percent of PSGP funding building new capability" and "Percent of PSGP funding sustaining existing capability," depicted in Table 1. FEMA does not set targets for percentage of funding applied to sustaining existing capabilities over building new capabilities as it believes the grantees and the Captains of the Port are in the best position to determine such priorities. Despite a reduction in PSGP funding of 49 percent and 51 percent in FY's 2012 and 2013, respectively, compared to FY 2011, these measures demonstrate that PSGP grantees have continued to build new capabilities. In FY 2013, 53 percent of PSGP funding was awarded to projects building new capabilities to reduce identified port security gaps and vulnerabilities. PSGP funded investments to strengthen the Nation's critical infrastructure against risks associated with potential terrorist attacks by closing identified capability gaps and USCG identified security vulnerabilities.

*Table 1. PSGP Programmatic Performance Measure*

Performance Measure	Description	FY 2013 Results
Percent of PSGP funding building new capability	This data is collected at the project level and represents the percent of funding supporting projects to reduce identified security gaps and vulnerabilities.	53%
Percent of PSGP funding sustaining existing capability	This data is collected at the project level and represents the percent of funding supporting projects that sustain existing capabilities	47%

<b>Question#:</b>	1
<b>Topic:</b>	PSGP 1
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

FEMA's Grant Programs Directorate (GPD) has also developed management and administrative performance measures to help strengthen the implementation, administration, and oversight of the PSGP. FEMA tracks, annually, these performance measures on award processing, financial and programmatic monitoring, and grant award closeout. Below are results for FY 2012 and 2013.

Data collection for FY 2014 is still ongoing at this time.

*Table 2. GPD Management and Administrative Performance Measures*

Performance Measure	Description	FY 2012 Results	FY 2013 Results
Percent of preparedness grant awards processed within 120 days	This measure determines the efficiency in which GPD processes preparedness grant awards.	100%	100%
Percent of preparedness grant awards monitored programmaticaly	This measure determines the percentage of preparedness grant awards monitored for consistency with the grantees' stated implementation plans and according to applicable rules and regulations.	11%	100%
Percent of preparedness grant funds monitored programmaticaly	This measure determines the percentage of available grant funds monitored for consistency with the grantees' stated implementation plans and according to applicable rules and regulations.	29%	100%
Percent of grant funds released to grantees within 270 days	This measure determines the efficiency in which GPD releases preparedness grant funds and assists grantees in meeting award conditions.	91%	95%
Percent of preparedness grant awards closed within 90 days	This measure determines the efficiency in which GPD is able to close-out grant awards after grantees have completed all administrative activities and related work.	48%	42%

FEMA continues to work with the USCG to develop and implement comprehensive outcome measures to further monitor the effectiveness of the PSGP.

<b>Question#:</b>	2
<b>Topic:</b>	PSGP 2
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Coast Guard uses the Maritime Security Risk Analysis Model (MSRAM) to assess maritime security risk, which produces a risk index number (RIN) for each maritime target, such as a shipping terminal or passenger ferry, that allows Coast Guard officials at the local, regional, and national levels to compare and rank critical infrastructure for the purpose of informing security decisions. Have you considered incorporating completed security projects into the vulnerability component of the risk model and annually update to provide accurate information to the PSGP formula to determine port tiering?

**Response:** Each year the Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA) and the United States Coast Guard (USCG) work collaboratively to review and update the results of the Maritime Security Risk Analysis Model (MSRAM) tool as it relates to the Port Security Grant Program (PSGP) Risk Model. In Fiscal Year (FY) 2011, DHS introduced a more robust vulnerability component to the Risk formula. DHS/FEMA has considered incorporating more data sets from the MSRAM tool, such as data "related to completed security projects" into the formula. The formula as a whole, including the vulnerability component, are reevaluated and refreshed annually or as needed. However, a final determination/decision for inclusion of this specific data, or any new more comprehensive components, remains undetermined but a viable option for consideration by the USCG, DHS Intelligence and Analysis, and FEMA.

Completion of long term capital projects associated with PSGP will account for a reduction of overall risk, depending on the type of project, and the MSRAM data collection criteria and methodology include aspects related to vulnerability. Therefore, over time, the completion of security related projects addressing vulnerability would be reflected in the MSRAM analysis and impact the risk index number. As FEMA is a customer of data provided by USCG's analysis, the relative increase or decrease in vulnerability of MCIKR/attack mode pairs, would best be articulated by the USCG through data provided in MSRAM reports. Finally, FEMA and the USCG continue to look at ways to further enhance the PSGP risk model and will again revisit all options for the FY 2015 grant cycle.

<b>Question#:</b>	3
<b>Topic:</b>	Risk
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Risk model consists of three variables: threat (the relative likelihood of an attack occurring), vulnerability (the relative exposure to an attack), and consequence (the relative expected impact of an attack). Has any of the “Risk” been bought down? Are there any mechanisms in place to make this determination? How can the Coast Guard’s Maritime Security Risk Analysis Model (MSRAM) be utilized to develop performance metrics? How can the Threat and Hazard Identification and Risk Assessments (THIRA) be utilized to develop performance metrics?

**Response:** Since its inception, the Port Security Grant Program (PSGP) has been consistent in its purpose, goals, and objectives for reducing risk at our Nation’s ports. Generally, port-grant funding must address specific maritime security priorities as identified by the United States Coast Guard (USCG), the Federal Emergency Management Agency (FEMA), and other Department of Homeland Security components. There are currently six security priorities, Cyber Security being the most recent addition (in FY 2013). The other priorities include: Enhancing Maritime Domain Awareness; Enhancing Improvised Explosive Devices (IED) and Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) prevention, protection, response, and recovery capabilities; Port Resilience and Recovery Capabilities; Training and Exercises; and Equipment Associated with Transportation Worker Identification Credential Implementation.

PSGP projects also support the development and sustainment of the core capabilities in the National Preparedness Goal. Further, PSGP funds support a port area’s Area Maritime Security Plan, a port area’s Facility Security Plans, and a port area’s Vessel Security Plans. These support the overall goals of the Maritime Transportation Security Act and the port area’s Port-Wide Risk Mitigation Plan.

Since its inception, PSGP funding has allowed for the closure of critical gaps in port security. The funding has enhanced overall Maritime Domain Awareness by contributing to improved port area surveillance and communications systems; improved facility security and hardening through the use of physical barriers and access controls; and enhanced CBRNE and IED prevention, protection, response, and recovery capabilities. PSGP funds have supported the purchase of specialized patrol vessels, specialized response vehicles, and equipment to further increase security of critical infrastructure in our ports and waterways. PSGP funding also has been instrumental in supporting planning, training, and exercises.

<b>Question#:</b>	3
<b>Topic:</b>	Risk
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

FEMA's strategy for evaluating grant performance in "buying-down" risk begins with National Preparedness Goal. Communities set their individualized, specific and measurable capability targets for the core capabilities defined in the Goal through the Threat and Hazard Identification and Risk Assessment (THIRA) process FEMA outlined in Comprehensive Preparedness Guide 201: THIRA Guide, Second Edition. Although ports receiving PSGP funding are not required to complete a THIRA, Urban Areas receiving funding under the Urban Areas Security Initiative (UASI) Grant Program must complete a THIRA. In 2013, 18 of the 25 Urban Areas eligible for 2013 UASI grant funding included port entities that received PSGP awards. Of these 18 Urban Areas, 11 reported to FEMA that port agencies participated in the Urban Area THIRA development.

While Urban Areas produce their own THIRAs, they provide their information to their respective state for inclusion in statewide THIRAs and State Preparedness Report (SPR). States use information from the UASIs, port entities, and other whole community partners to assess their current capability levels against statewide capability targets in their annual SPRs. Taken together, the THIRA and the SPR identify capability needs and gaps. Using THIRAs and SPRs, FEMA tracks the closing of gaps and the improvement against capability targets.

FEMA and the USCG target critical port security funds where they are most needed. Using its Maritime Security Risk Analysis Model (MSRAM), the USCG assesses the relative risks of terrorist attacks against maritime critical infrastructure and key resources. MSRAM data is one of the components, accounting for the National Infrastructure Index of the FEMA/DHS Risk Allocation Formula that informs PSGP allocations and funding decisions.

MSRAM has been accredited and applied by the USCG to specifically analyze threat, vulnerability and consequence at individual critical infrastructure and key resources. The model was not designed to analyze results from port-wide projects or multiple projects across a port and accordingly, MSRAM would not be appropriate for developing performance metrics for PSGP.

The THIRA process is a means by which grantees, such as those receiving PSGP funding, could develop performance measures. A fundamental step in the THIRA process, after identifying threat and hazards of concern and giving those threats and hazards context, is to set capability targets for the threats and hazards particular to a given community. The capability targets are specific and measurable statements of success for each of the 31 core capabilities. These specific, measurable capability targets can be used to support port-focused performance metric for each of the core capabilities.

<b>Question#:</b>	3
<b>Topic:</b>	Risk
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Coordination with state and Urban Areas in the THIRA process is critical to ensure that the threats and hazards and capability targets represent whole community partners, to include ports.

**Post-Hearing Questions for the Record  
Submitted to Stephen Sadler  
From Senator Tom A. Coburn, M.D.**

**Evaluating Port Security: Progress Made and Challenges Ahead**

**June 4, 2014**

<b>Question#:</b>	1
<b>Topic:</b>	TWIC program
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The TWIC program is in its 12th year, more than \$453 million (according to most non-governmental sources) has been spent on the program and TSA has issued over 2.4 million active cards, yet program implementation is not yet complete. Why is this program not completed? What are the challenges that have delayed this complete implementation? When will the program be completely implemented?

**Response:** The Transportation Worker Identification Credential (TWIC) Program is a joint program managed by both the Transportation Security Administration (TSA) and the United States Coast Guard (USCG), which includes the issuance of a TWIC for unescorted access to secure areas within Maritime and Transportation Security Act (MTSA)-regulated facilities and the effective use of readers for access control. TSA completed the implementation of the enrollment, processing and card production part of the program in 2007 and the first TWIC was issued in October 2007. The second requirement of the program is for USCG to provide guidance and direction for the use of readers across MTSA-regulated facilities and vessels. As such, the USCG published the TWIC Reader Requirements Notice of Proposed Rulemaking (NPRM) on March 22, 2013. The NPRM proposes the use of TWIC readers by MTSA-regulated vessels and facilities that pose the greatest risk—38 vessels and 532 facilities—and maintains the visual verification requirement for remaining vessels and facilities. The comment period for the TWIC Reader Requirements NPRM was open until May 21, 2013, and included four public meetings hosted by the USCG. The 2013 public meetings occurred on:

- o April 18 in Arlington, VA,
- o April 25 in Houston, TX,
- o May 2 in Seattle, WA, and
- o May 9 in Chicago, IL

<b>Question#:</b>	1
<b>Topic:</b>	TWIC program
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

The NPRM proposes a full 2-year implementation period from the date of publication of the Final Rule for the affected population to reach full compliance. It is anticipated that the Final Rule will be published in early 2015.

<b>Question#:</b>	2
<b>Topic:</b>	TWIC cards 1
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Department of the Navy, until March of 2014 allowed the use of TWIC cards to gain access to its facilities, made changes adding a National Crime Information Center database check prior to gaining access to its facilities following the USS MAHAN shooting at Naval Station Norfolk. Jeffrey Tyrone Savage, the shooter at the Norfolk Navy facility, had received a TWIC in January of 2014.

Why was Savage issued a TWIC after recently serving 552 days for a felony manslaughter charge and 5 additional years for selling illegal drugs?

**Response:** At the time of Mr. Savage's eligibility review for a Transportation Worker Identification Credential, his drug conviction was not disqualifying because it occurred outside the timeframes established in the governing statute. Also, at that time, the Transportation Security Administration's (TSA's) policy did not consider manslaughter a disqualifying offense. Following this incident, TSA re-evaluated the adjudication procedures and policies and now treats voluntary manslaughter as an interim disqualifying offense.

Note that a TWIC alone does not authorize or guarantee access to a maritime facility that is governed by the Maritime Transportation Security Act. Rather the TWIC establishes an individual's eligibility to enter, and the individual must show a business need to enter before being granted access. Individuals must have a business need to enter the facility or port and be approved for entry by the facility. Each port facility or vessel may establish additional requirements for entry. In the case of Mr. Savage, he did not have a business need to enter, was not granted access to the facility, and his TWIC was not used to access the base.

**Question:** Why did TSA choose not to use the authority under (section 49 CFR 1572.107) that allows the Administrator to deny a TWIC where there is an extensive record of serious crimes that may not include a listed disqualifying offense, incarceration for more than 365 days, and other factors?

**Response:** At the time of Mr. Savage's eligibility review for a TWIC, TSA policy did not consider Mr. Savage's criminal history for further review under 49 CFR 1572.107. Following the incident in Norfolk, Virginia, TSA re-evaluated its adjudication procedures and policies, and developed new adjudication standards to account for extensive criminal histories that may fall outside the list of specific crimes and timeframes set forth in the

<b>Question#:</b>	2
<b>Topic:</b>	TWIC cards 1
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

governing list of disqualifying offenses in 49 CFR 1572.103, but may be considered disqualifying under 49 CFR 1572.107.

<b>Question#:</b>	3
<b>Topic:</b>	criminal information
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** TSA's inability to access updated criminal information about a TWIC holder between the time a TWIC is issued and its renewal five years later (unless the information is self-reported). The Security Clearances program is having similar issues and both are very dangerous to national security, what changes are being made to TSA's comprehensive Security Threat Assessment (TSA) to address this very serious concern? What coordination or information does TSA need to quickly improve the vetting process?

**Response:** The Transportation Security Administration (TSA) is continually reviewing its policies, procedures, and regulations governing the eligibility standards for the Transportation Worker Identification Credential (TWIC) program, including criminal history.

It is important to note that under current Federal Bureau of Investigation (FBI) policy, the security threat assessments that TSA conducts are considered to be for non-criminal justice purposes, and as such, TSA is not authorized to conduct name-based, recurrent criminal history records checks. Recurrent checks must be accompanied by a re-submission of fingerprints and an additional fee to cover the FBI's costs for conducting the new criminal check. It was determined during the TWIC rulemaking that conducting this check more than once every 5 years was not cost-beneficial. Thus, TSA's evaluation of an applicant with regard to criminal history is based on the applicant's history available at the time of enrollment. Currently, TSA can re-evaluate an individual's criminal history for TWIC eligibility when the individual applies to renew the TWIC 5 years after the original TWIC was issued.

The FBI is developing a notification process that would provide information to agencies that have submitted fingerprints for review if additional criminal history related to those fingerprints occurs. Later this year, the FBI intends to enhance its criminal history systems capabilities to begin to offer this notification opportunity to agencies for an additional fee. TSA has been working with the FBI to determine how to implement this capability and will update its procedures so that an individual's TWIC eligibility can be re-evaluated if new criminal history occurs.

<b>Question#:</b>	4
<b>Topic:</b>	TWIC computer server
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Recently, a former Navy systems administrator led a group that hacked into the TWIC computer server exposing cyber vulnerabilities, the Department of the Army in a 2013 response declared that TWIC could no longer meet the DoD security standards and denied its use to authenticate users for access to DoD systems. What measures have been taken to ensure that the highly confidential information kept by TSA is secure?

**Response:** The Transportation Worker Identification Credential (TWIC) system was not the target nor the victim of the hacking incident listed in the question. Rather, it was a support website ([twicinformation.tsa.dhs.gov](http://twicinformation.tsa.dhs.gov)) maintained by a contractor that contained enrollment center locations and hours of operation. No Personally Identifiable Information (PII), Sensitive Security Information (SSI), login information, or any other sensitive information was hosted on that website.

The Department of the Army decision relates to individuals accessing the Department of Defense (DoD) ETA system. The TWIC card is issued to private sector workers and was never intended to be used for “logical” access to secure DoD computer systems. The DoD continues to formally recognize the TWIC card as an acceptable credential for physical access to DoD facilities with a valid business case.

Within the past few years, both the Internet facing front end and the processing back end of the TWIC system have been completely replaced with a more modern infrastructure with enhanced security features. The Universal Enrollment System (UES) is the new Internet facing system, and the Technology Infrastructure Modernization system is the new back end processing infrastructure. The UES system acquired an Authority to Operate (ATO) in December 2012, and TIM acquired an ATO in March 2014. As part of this ATO process, there are continuous monitoring monthly scans of the systems and annual assessments of technical, operational, and management controls. In addition, all applicant and Security Threat Assessment (STA) data captured and stored throughout these systems is fully encrypted and is transmitted using PKI and certificate authentication in all interfaces.

<b>Question#:</b>	5
<b>Topic:</b>	TWIC cards 2
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** TSA has a database that updates the canceled TWIC cards to ensure that access is limited to individuals with active and accurate TWICs. However the database is not accessible by ports, but can be printed daily by the port at the TWIC website <https://universalenroll.dhs.gov/>. Do you believe it is feasible to require any port, vessel or facility to go through 1800 pages to validate the TWIC credential? What is TSA doing to address is issue?

**Response:** The Cancelled Card List (CCL) is updated daily and available on a 24x7 basis for download from the internet to allow the ports to integrate with their respective physical access control systems and procedures. With access to the CCL, the ports can electronically query the CCL to determine if an individual's Transportation Worker Identification Credential (TWIC) is on the list through the Federal Agency Smart Credential Number loaded electronically on the card. It is not necessary to print the CCL for manual review.

<b>Question#:</b>	6
<b>Topic:</b>	TWIC and the Hazmat Endorsement
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The TWIC and the Hazmat Endorsement (HME) are redundant credentialing programs administered by TSA. Both programs query the same databases for criminal, immigration, and other violations, utilizing the same disqualifying criteria, appeal, and waiver processes. ? ? ? How much money (in fees) would be lost by TSA?

Why are the TWIC and Hazmat Endorsement credentials separate?

**Response:** Under the current statutory regime, states are required to issue the hazardous materials endorsement (HME) on a commercial driver's license (CDL), and the Transportation Security Administration (TSA) is required to issue the Transportation Worker Identification Credential (TWIC).

The USA PATRIOT Act prohibits states from issuing an HME in commerce unless TSA has determined that the individual does not pose a security risk. In addition, under transportation laws and regulations, states must apply certain training and safety standards before issuing the HMEs. TSA issued standards to implement its portion of the HME program and conducts a security threat assessment (STA) on anyone applying to obtain, renew, or transfer an HME on their state-issued commercial driver's license (CDL). TSA notifies the state of its security determination and then the state may issue the HME to those who pass the STA and comply with state training and safety requirements.

The Maritime and Transportation Security Act (MTSA) requires TSA to conduct an STA and issue a biometric credential for transportation workers who must have unescorted access to MTSA-regulated ports and vessels. TSA issued standards to implement these requirements and conducts an STA on anyone applying to obtain or renew a TWIC and issues the credential to those who pass the STA.

**Question:** Do they require the same background check procedures?

**Response:** In accordance with the pertinent statutes and regulations, the STAs for the HME and TWIC are comparable. However, the credential issuance process differs due to statutory requirements.

**Question:** What would be the cost savings if the two credentialing programs were combined?

<b>Question#:</b>	6
<b>Topic:</b>	TWIC and the Hazmat Endorsement
<b>Hearing:</b>	The Security and Accountability For Every (SAFE) Port Act
<b>Primary:</b>	The Honorable Tom A. Coburn
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Response:** Due to the statutory requirements governing the issuance of HMEs on CDLs, the TWIC and HME programs cannot be fully combined. However, TSA has worked to reduce fees and eliminate redundant STAs with these programs. The transportation worker does not have to complete a new STA or pay for a new STA if they have an existing, valid STA in a comparable program. Currently, if an HME holder applies for a TWIC, he or she does not have to complete a new STA or pay the fee for the STA to obtain the TWIC. If a TWIC holder applies for an HME, he or she may leverage the TWIC STA in states that have the capability to verify that the TWIC STA remains valid. Twenty-four states and the District of Columbia currently have the capability to offer this comparability to TWIC holders applying in their state for an HME. Under the TSA Universal Enrollment Services and Technology Infrastructure Modernization (TIM) program, comparability will be applied where feasible, as well as provide the capability for individuals to enroll in multiple programs at the same time.

**Question:** How much money (in fees) would be lost by TSA if the credentialing programs were combined?

**Response:** TSA is required by Congress to collect user fees to cover the cost of vetting and credentialing. TSA does not lose fees for providing comparability. When TSA completes an STA, it collects the cost of that service from the applicant. If TSA does not conduct a new STA, there is no need to collect a fee because no service has been completed. TSA currently provides comparability between the TWIC and HME programs; therefore, TSA does not need to complete a new STA where the applicant has an existing, valid STA.

**Question:** What other credentialing programs is TSA responsible for.

**Response:** TSA issues a physical credential only for the TWIC program. However, TSA is responsible for a variety of transportation vetting programs in aviation and surface transportation sectors, including: Alien Flight Student Program, Airport Workers, Flight Crew Vetting, Air Cargo Operations, Indirect Air Carriers, Federal Aviation Administration Certificate Holders, Private Charter Operations, and 12/5.

**Question:** Can you provide the number of TWIC holders that hold multiple credentials that require an additional TSA screening process?

**Response:** In calendar year 2014, approximately 2,500 transportation workers, or 1 percent of individuals applying for a TWIC, have an existing, valid STA and do not require additional screening until they apply for reenrollment.