BALANCING MARITIME SECURITY AND TRADE FACILITATION: PROTECTING OUR PORTS, INCREASING COMMERCE AND SECURING THE SUPPLY CHAIN—PART I

HEARING

BEFORE THE

SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

FEBRUARY 7, 2012

Serial No. 112–65

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

76–511 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
JACKIE SPEIER, California
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

CANDICE S. MILLER, Michigan, *Chairwoman*

MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
PAUL C. BROUN, Georgia
BEN QUAYLE, Arizona, *Vice Chair*
SCOTT RIGELL, Virginia
JEFF DUNCAN, South Carolina
PETER T. KING, New York *(Ex Officio)*

HENRY CUELLAR, Texas
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
BRIAN HIGGINS, New York
HANSEN CLARKE, Michigan
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

PAUL ANSTINE, *Staff Director*
DIANA BERGWIN, *Subcommittee Clerk*
ALISON NORTHROP, *Minority Subcommittee Director*

CONTENTS

BALANCING MARITIME SECURITY AND TRADE FACILITATION: PROTECTING OUR PORTS, INCREASING COMMERCE AND SECURING THE SUPPLY CHAIN—PART I

Tuesday, February 7, 2012

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

The subcommittee met, pursuant to call, at 10:03 a.m., in Room 311, Cannon House Office Building, Hon. Candice S. Miller [Chairwoman of the subcommittee] presiding.

Present: Representatives Miller, Broun, Duncan, Cuellar, Sanchez, Jackson Lee, Clarke of Michigan, and Thompson.

Also present: Representatives Richardson and Hahn.

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

The subcommittee is meeting today to hear testimony from Congressman Jerry Nadler, from assistant secretary David Heyman, from Department of Homeland Security Office of Policy, acting assistant commissioner Kevin McAleenan, Office of Field Operations, Customs and Border Protection, Rear Admiral Paul Zukunft—I know I am never pronouncing that correctly, assistant commandant for marine safety, security, and stewardship with the U.S. Coast Guard, and Mr. Steve Caldwell, who is the director of Maritime Security from GAO.

Today our very important topic is the global supply chain. I would recognize myself for an opening statement.

This hearing is really the first of a two-part series. We are going to have another follow-on hearing as well. We are going to examine the Nation's maritime and global supply chain security measures.

Last year, this subcommittee focused on security at the Southern and the Northern Border, both at and between the ports of entry. But I think it is important as well to remember that we really have three borders.

The Nation's maritime border is certainly just as important as the other two. It is a conduit for much of the country's trade. Commerce, of course, is the life blood of the Nation.

After September 11, we in the Congress rightly recognized the importance of securing our Nation's ports and the cargo that transits from overseas to our stores and our shops here on a daily basis.

I have actually had the opportunity recently really to visit some of our Nation's largest ports and see first-hand the hard work that the men and women of Customs and Border Protection and the United States Coast Guard do to help secure our Nation.

However, it is certainly clear that more work needs to be done. Whether it comes into our ports or travels by truck, coming through Laredo or El Paso or what have you, or coming across from a train from Canadian border, we have to always make sure that we understand the risk posed by cargo shipment in order to secure the entire global supply chain.

The logistics involved in moving goods across the global supply chain are incredibly complex. Security solutions we propose should be cognizant of that reality.

Today's hearing will examine how we balance maritime security and the safeguarding of our supply chains with the need to facilitate trade and not place an undue burden on a flow of goods that is so vital to our way of life.

Delays to shipping can cost billions of dollars to our economy. Balancing security and facilitating commerce is not an easy thing. But risk-based systems and trusted trade programs can help separate companies who play by the rules and make extra efforts, allowing the Customs and Border Protection to focus on less-secure shipments.

We need to make sure that we push our borders out by conducting as much of CBP's cargo inspection and screening work before potentially dangerous cargo arrives on our shores.

We can and we must do a better job of leveraging the work of our trusted allies to help screen and, when necessary, either scan or inspect high-risk cargo. It is no secret that our Nation faces a difficult financial situation. We are always going to have limited taxpayer dollars.

That requires that the Government make smart decisions to use those resources in the most effective and efficient possible manner. We should be under no illusion that we can eliminate every single risk, certainly, that terrorists pose to the Nation, and that all we need to do is just to spend more to make that risk completely disappear.

A clear-eyed assessment of risk should inform how we allocate scarce Homeland Security dollars as well.

I think this is especially important to remember when considering the 9/11 Act, which mandated 100 percent screening—or excuse me, scanning of cargo prior to it arriving in America.

Certainly that is a very, very worthwhile goal. That should be our goal.

However, we have to look at how we implement this law, whether it is possible, the potential costs, and the benefits as well.

We currently scan 4 to 5 percent of all containerized cargo entering the country, based upon the National Targeting Center's data screening system and the current threat environment.

It is certainly far from clear that the investment required to scan the rest of the 95 percent of the cargo is possible, is wise. Again, we are going to be talking about based on risk; is it grounded in a proper understanding of the threat posed by containerized cargo?

The Secretary, herself, of the Department of Homeland Security has mentioned on numerous occasions, including in front of this committee, on a number of times that she wants to work with the Congress to modify this requirement. So I would say certainly I stand, and I know this committee stands ready to work with her.

We are waiting for her legislative proposal that will help move the country into a more risk-based system, as the Secretary has been saying now for over 2 years.

As part of our discussion today, I am eager to hear the witnesses' thoughts on the Customs Trade Partnership Against Terrorism, the C–TPAT Program. The private sector has a role to play in helping to secure their supply chains.

I think it is important to spend Customs and Border Protection officers' time on shippers of concern, rather than on trusted embedded companies, who are willing to make security enhancements. C–TPAT, you know, I think is a wonderful example, that program, of how Government and the private sector can really partner together to help increase security and ensure the smooth flow of goods.

We want to explore ways to improve and expand this program to additional companies that are willing to improve the security of the supply chain.

Then finally, I would like to note that the SAFE Port Act of 2006 calls for a global supply chain strategy to be released. This requirement came due in October 2009, but actually was not released until just a few days ago—excuse me, a few weeks ago.

I think it is interesting to note that many times this subcommittee has been having hearings on particular issues, and then the agency, the Department responds, which I think is a very good thing. In fact, we held a hearing in July on maritime cooperation; and then the Department released their Maritime Coordination Plan, right at that time.

Then we held a hearing on visa security in September; and the Department released an announcement on visa security on the day of our subcommittee hearing. So I don't know if it is serendipity or what, but I think it is great.

The Congress is doing its job on oversight. The agencies are responding. I think that tells us that this subcommittee is focused on the right issues, matters of security for our Nation as well.

However, I will mention that even though we just received this a couple of weeks ago, the document that was produced by the White House, it is only 6 pages long. The first page was an executive summary.

So I am certainly looking forward to hearing the Department's plans on the implementation details, and their complete vision on a strategy that will help us better secure the supply chain.

With that, I would also like to recognize now the Ranking Member of the subcommittee, gentleman from Texas, Mr. Cuellar, for his opening remarks.

[The statement of Chairwoman Miller follows:]

STATEMENT OF CHAIRMAN CANDICE S. MILLER

FEBRUARY 7, 2012

This hearing is the first of a two-part series that will examine the Nation's maritime and global supply chain security measures.

Last year this subcommittee focused on security at the Southern and Northern Border, both at and between the ports of entry, but I think it is important to remember that we have three borders. The Nation's maritime border is just as important as the other two, and is the conduit for much of the country's trade. Commerce is the life-blood of the Nation, and after September 11 we in Congress rightly recognized the importance of securing our Nation's ports and the cargo that transits from overseas to our stores on a daily basis.

I recently had the opportunity to visit some of our Nation's largest ports and saw first-hand the hard work that the men and women of Customs and Border Protection and the U.S. Coast Guard do to help secure the Nation—however it is clear that more work needs to be done.

Whether it comes into the ports of Los Angeles and Long Beach, travels by truck through Laredo or on a train across the Canadian Border, we must correctly gauge the risk posed by cargo shipments in order to secure the entire global supply chain. The logistics involved in moving goods across the global supply chain is incredibly complex—security solutions we propose should be cognizant of that reality.

Today's hearing will examine how we balance maritime security and the safeguarding of our supply chains with the need to facilitate trade and not place an undue burden on the flow of goods that is vital to our way of life. Delays to shipping can cost billions of dollars to our economy. Balancing security and facilitating commerce is not an easy task, but risk-based systems and trusted trade programs can help separate companies who play by the rules and make extra efforts—allowing Customs and Border Protection to focus on less secure shipments.

A disruption or attack at one of our Nation's largest ports could be catastrophic, and we need to make sure we "push the borders out" by conducting as much of CBP's cargo inspection and screening work before potentially dangerous cargo arrives on U.S. shores. We can and must do a better job of leveraging the work of our trusted allies to help screen, and when necessary, scan or inspect high-risk cargo.

It is no secret that the Nation faces a difficult financial situation—we will always have limited taxpayer dollars and that requires that the Government make smart decisions to use those resources in the most effective and efficient manner possible. We should be under no illusion that we can eliminate every single last ounce of risk that terrorists pose to the Nation and that all is needed is to spend more to make that risk completely disappear. A clear-eyed and sober assessment of risk should inform how we allocate scarce homeland security dollars—we just don't have the resources to do it any other way.

I think this is especially important to remember when considering the 9/11 Act, which mandated 100% scanning of cargo prior to it arriving in America. Let me be clear—I think this is a worthwhile goal; however, we must look at the impediments to the implementation of this law, such as potential costs and benefits. We currently scan 4–5 percent of all containerized cargo entering the country based upon the National Targeting Center's data screening system and current the threat environment. It is far from clear that the investment required to scan the rest of the 95% of cargo is wise, is based on risk, or is grounded in a proper understanding of the threat posed by containerized cargo.

The Secretary herself has mentioned on numerous occasions, including in front of this committee that she wants to work with the Congress to modify this onerous requirement. Today, I stand ready to work with her, and I await her legislative proposal that will help move the country into a more risk-based system, as the Secretary has been saying for almost 2 years.

As part of our discussion today, I am eager to hear the witnesses' thoughts on the Customs Trade Partnership Against Terrorism (the C–TPAT program). The private sector has a role to play in helping to secure their supply chains, and I think it is important to spend Customs and Border Protection officer's time on shippers of concern, rather than on trusted and vetted companies who are willing to make security enhancements. C–TPAT is an example of how Government and the private sector can partner together to help increase security and ensure the smooth flow of goods. I want to explore ways to improve and expand this program to additional companies that are willing to improve the security of the supply chain.

Finally, I would like to note that the SAFE Port Act of 2006 called for a global supply chain strategy to be released. This requirement came due in October 2009 but was not released until just a few weeks ago. I am disappointed that this document produced by the White House provided little more than high-level concepts and did not articulate a tangible path forward. More than 27 months late and a grand total of 6 pages; it is nothing short of an embarrassment. Is this really the best we could do? I look forward to hearing DHS' plans on the implementation de-

tails and their complete vision for this strategy can lead to a more secure supply chain.

Mr. CUELLAR. Thank you so much, Madam Chairwoman, for holding this meeting.

Also I would like to recognize our Ranking Member of the full committee. Again, thank you for holding this meeting.

Madam Chairwoman, before I move forward with a statement, I would ask for unanimous consent to allow the gentle lady from California, Ms. Richardson and Ms. Hahn, both from California, to sit and question the witnesses in today's hearing.

Mrs. MILLER. Without objection.

Mr. CUELLAR. Thank you so much.

As you know, this subcommittee has previously examined cargo security and facilitation issues at our land borders. Some of our Nation's busiest land ports of entry are located in my Congressional district, making supply chain security and facilitation of legitimate commerce a key issue for me and my constituents.

I know this issue is of great importance to the gentle lady from Michigan as well, given her district along the Northern Border. I appreciate all the work that she has done there to make sure we facilitate finding the balance between security and, of course, commerce moving as quickly as possible.

Today, we are examining another important part, which is the maritime cargo security, that have certain parallels.

Indeed, the fundamental issue is the same: How can we expedite legitimate cargo to its destination, while keeping possible terrorist instruments or contraband from entering the United States? Given the volume of cargo crossing and entering this country every day, this is no easy task for DHS and its settled partners.

We are hearing testimony today regarding DHS programs and initiatives to secure maritime cargo, through programs such as the Container Security Initiative, Secure Freight Initiative, and the C–TPAT.

I have also had the opportunity to visit a TSI port with Mr. Thompson. I have also been to the National Targeting Center, where much of the Customs and Border Protection cargo security work is done.

While I appreciate the hard work of the men and women of CBP and their DHS colleagues on this challenging issue, more remains to be done. Many of the cargo security programs have grown stagnant in recent years, in part due to lack of adequate funding.

Many of those programs are carried out by CBP officers who are in short supply. We have greatly expanded the ranks of the Border Patrol, the men and women in green, since September 11, 2001. But we have not kept pace with the CBP officers, the men and women in blue.

We need to do better to make sure that we get the men and women in blue, because those are the ones that man our airports, our seaports, and our land ports. Without adequate personnel, our sea, land, and airport security and facilitation will both suffer.

Finally, I would like to bring also the issue that Madam Chairwoman also brought up, which is my dismay at the recently released, long-overdue National Security and Supply Chain Security.

This was due in 2009. It just got released this last month, in January.

Again, not that weight counts or number of pages counts, but 6 pages I think is not sufficient for such a very important issue that we have here. I am hoping that we will get a little bit more substance from the administration on the path forward for supply chain security and facilitation.

I know we can do better than this. It is my hope that the witnesses today will be able to speak to DHS' vision for its role in this very important mission.

I thank the witnesses for joining us here today. I look forward to your testimony.

With that, Madam Chairwoman, I yield back the balance of my time.

Mrs. MILLER. Thank the gentleman.

The Chairwoman now recognizes the Ranking Member of the full committee, the gentleman from Mississippi, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Madam Chairwoman. I appreciate you calling this hearing. I appreciate our witnesses for their participation also.

Today's hearing comes at a critical juncture in the Department of Homeland Security's efforts to secure maritime cargo entering our Nation's ports. Later this year, July 12, 2012, marks the deadline for achieving 100 percent scanning of maritime cargo before it arrives in the United States, pursuant to the implementation recommendation of the 9/11 Commission Act 2007.

In other words, the law requires all U.S.-bound cargo be scanned either through non-intrusive scanning machines, or receive a physical examination. Today, it is widely acknowledged that DHS will not meet this deadline.

I am a pragmatic person. I was a proponent of 100 percent scanning mandate, but understood that fulfilling the requirements would be no easy task. However, those of us who supported the provision hoped to spur significant advances in cargo security by this point, even if the initial 2012 deadline was not met.

Instead, in the nearly 5 years since the law was enacted, DHS has failed to make an honest effort to implement the mandate. We have heard a litany of reasons that 100 percent scanning cannot or should not be done.

In testimony before this committee, Secretary Napolitano expressed opposition to the mandate, indicating that the 100 percent requirement is not achievable by 2012, and instead advocating for a risk-based approach to maritime cargo security.

Of course, the surest way to fail is not to try at all. Equally troubling is the fact that in recent years, some of DHS' existing cargo security programs have become stagnant or have been scaled back.

For example, the Container Security Initiative, CSI, is operational in the same 58 ports that were active before the enactment of the 9/11 Act. Over the past 5 years, CSI has not been expanded, despite the fact that at least 700 ports ships goods to the United States. The number of overseas personnel deployed to the 58 ports has plummeted.

Specifically, in 2009, there were 167 CSI officers at overseas ports. Today, there are only 79. Similarly, while a few years go, the

Secure Freighter Initiative included six ports, today, the program has reduced to a single low-volume port.

Last month, the administration released a long-awaited "National Strategy for Global Supply Chain Security." You have heard my Ranking Member talk about the size of this 6-page document. It is hard to see how this document could offer a comprehensive blueprint for enhancing the security of the supply chain, especially given the enormity of the task and the number of stakeholders involved.

Nevertheless, I expect to hear testimony today from DHS witnesses about how successful the Department has been at creating programs to ensure that shippers can be trusted, manifest, or analyzed, and ports are protected. These programs play an important role in maritime security.

However, they do not take the place of having an active partnership, where CBP personnel work with their foreign counterparts in overseas ports to examine high-risk cargo containers before they arrive in U.S. ports.

After all, what good is identifying a high-risk container if it doesn't get examined until it has arrived in the Ports of New York, Houston, Los Angeles, New Orleans or any of the other hundreds of ports across America?

By then, it very well may be too late.

I hope to hear from our witnesses today not only about the successes, but also about what remains to be done to secure maritime cargo, and how we can get there. Meaningful homeland security will only be achieved when we know who and what is coming into this country, not only by air and land but also by sea.

I thank the witnesses for joining us today, Madam Chairwoman. I look forward to their testimony.

Mrs. MILLER. Thank the gentleman.

I would remind all the other committee Members as well that opening statements that you may have can be submitted for the record.

[The statement of Hon. Richardson follows:]

STATEMENT OF HON. LAURA RICHARDSON

FEBRUARY 7, 2012

I would like to thank Chairwoman Miller and Ranking Member Cuellar for allowing me to participate in today's subcommittee hearing. I look forward to hearing from our distinguished panel of witness on how we can increase commerce through our ports, while protecting our ports against a terrorist attack. I am particularly interested in hearing how the Department of Homeland Security will address the law that requires 100 percent of containers be scanned prior to arrival in the United States by July 12, 2012.

After the terrorist attacks on September 11, 2001, the 9/11 Commission was established to help protect our country against future attacks. One of the Commission's recommendations was that all cargo containers be scanned prior to being loaded on a vessel bound for the United States. The Implementing Recommendations of the 9/11 Commission was signed into law on August 3, 2007. This law required that the Secretary of Homeland Security meet the mandate of 100 percent container scanning by July 12, 2012, unless the Secretary extends the deadline by certifying that it is currently not feasible.

Unfortunately, DHS has made little effort in meeting this mandate. I have consistently raised this extremely important National security issue with the Department of Homeland Security.

- At a full Homeland Security Committee hearing on February 25, 2010, I questioned Secretary Napolitano on the Department's progress towards the 100 percent container screening mandate.
- On June 16, 2010, as Chairwoman of the Subcommittee on Emergency Communications, Preparedness, and Response, I and the other Homeland Security Committee chairs sent a letter to Secretary Napolitano regarding the Department's policy and efforts to meet the 2012 deadline.
- At a full Homeland Security Committee hearing on March 3, 2011, I again questioned Secretary Napolitano on the 100 percent container screening law. The Secretary responded that the 100 percent mandate was constructed at a time before there was a mature understanding of what the possibilities were in the maritime cargo security and that the Department was working on an entire "global cargo security initiative" that involves the International Maritime Organization, the International Aviation Organization, and the World Customs Organization.

The Department of Homeland Security has given multiple reasons why the 100 percent container screening requirement will not be met. We have heard that the technology is not available, the costs of implementing the requirement is too high, it would cause delays in the global chain, there is not buy-in from foreign partners, and that the DHS is moving towards only screening 100 percent of high-risk containers. However, I am very concerned that DHS has not conducted any studies on the feasibility of meeting the 100 percent container screening mandate. DHS has also scaled back its maritime cargo security programs and reduced the number of personnel at overseas ports. I am also concerned that DHS has not made any efforts towards improving container screening, and will continue to extend the 100 percent container screening deadline without demonstrating a good faith effort in meeting the law's requirements.

Once cargo reaches our ports, it could be too late to prevent a catastrophic terrorist attack. The Port of Long Beach and the Port of Los Angeles are not only important to my district, but are also important to the U.S. and global economy. A nuclear or radiological bomb that detonated in the Port of Long Beach or the Port of Los Angeles would result in thousands of deaths and cripple our economy. We need to ensure that 100 percent of cargo that enters our ports is screened before they arrive.

In May 2011, I visited the Port City of Kaohsiung in Taiwan. I personally observed the screening process at this port. Kaohsiung screens 100 percent of containers prior to the being shipped to the United States. Suspicious cargo receives additional screening until it is cleared or removed for further investigation. We need to work with other countries to ensure this is happening before cargo is shipped to our U.S. ports.

A successful terrorist attack on one of our ports, such as the Port of Los Angeles or the Port of Long Beach would have a devastating economic impact and severely impact the global supply chain. The cost of one terrorist attack in our ports would far surpass the costs of instituting the 100 percent container scanning that is required by law and was recommended by the 9/11 Commission.

We have been extremely fortunate that an attack has not yet occurred in our ports. I was disappointed that the administration's National Strategy for Global Supply Chain Security did not address container scanning. As a Member of the Homeland Security Committee, I will continue to fight for the safety of our Nation's ports. Congress and the 9/11 Commission has made it clear that 100 percent container scanning is vital to our National security interests.

Again, I thank Chairwoman Candice Miller and Ranking Member Cuellar for allowing me to attend today's hearing. Port security is a top homeland security priority for me. I look forward from hearing from our DHS witnesses on what is being done to protect our ports against a terrorist attack. I also want to hear what is being done to ensure the safety of the containers that pass through our Nation's ports.

I yield back the balance of my time.

We are pleased to have two distinguished panels.

But our first panel is Congressman Jerry Nadler, who joins us today. We appreciate you, sir, coming. He represents the 8th District of New York, which includes much of the west side of Manhattan, the financial district, and a number of diverse neighborhoods in southwestern Brooklyn.

He began his political career in 1976 in the New York State Assembly, where he served for 16 years. Then in 1992, he was elected to the U.S. House of Representatives in a special election, has been here ever since.

With that, the floor is yours, sir. Again, we appreciate you taking time to give us your testimony and insight on this issue today.

STATEMENT OF HON. JERROLD NADLER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. NADLER. Thank you very much, Chairwoman Miller, Ranking Member Cuellar, Ranking Member Thompson, Members of the subcommittee.

Thank you for inviting me to testify today on the issue of maritime security and trade facilitation. I speak to you today not as a maritime cargo security expert, but as a Member of Congress who has long advocated that we as a Nation must do a better job of ensuring the security of the cargo arriving on our shores every day.

As representative from New York's 8th District. I have the honor of representing portions of Manhattan and Brooklyn. The World Trade Center site is located in my district, as is much of the Port of New York and New Jersey, the largest port on the East Coast.

As such, I believe my district stands as an example of why we need to secure our Nation, including our ports and waterways, while also ensuring the flow of legitimate commerce.

As you might recall, I was the principal author of many of the port provisions of the implementing recommendations of the 9/11 Commission Act of 2007. I worked closely with Chairman Thompson, then Chairman Oberstar, and Representative Ed Markey to push for inclusion of the 100 percent scanning provision into this measure.

We were successful. Section 1701 of that act states that by July 12, 2012, all cargo containers must be scanned by non-intrusive imaging equipment and radiation detection technology before being loaded on a vessel bound for the United States, unless the Secretary of Homeland Security extends the deadline by certifying it is not currently feasible.

In short, this provision requires scanning of all maritime cargo containers before they arrive in this country. We understood that we must not wait to impose security measures until containers reach the United States.

Scanning containers in the U.S. port is not sufficient. If there is a nuclear bomb inside a container and it is detected by radiation portal monitors in Newark or Miami or Los Angeles, it may very well be too late.

Reading the cargo manifests is not enough. Trusting certain shippers is not enough. We must verify the contents of the containers at the point of origin, before they are loaded on a ship bound for America.

So the law is designed to do just that.

When I introduced a free-standing bill on this topic, and later pushed for inclusion of these provisions in the 9/11 Act, I understood that achieving 100 percent maritime cargo scanning mandate would be neither easy nor cheap.

But I was also aware of the human and economic toll of a potential terrorist attack on our soil. The New York Metropolitan Area is home to approximately 19 million people. The effects of a weapon of mass destruction or a dirty bomb at the Port of New York or New Jersey would be catastrophic.

Similarly, several of the Nation's other major ports are located near populations—in fact, all of them are located near population centers, and might also make attractive targets for terrorists. This threat is not exclusive to major metropolitan areas, however.

There are currently approximately 360 commercial sea and river ports throughout the United States, making this issue of concern to communities across the country.

Aside from the potential human costs, the economic costs of a maritime terrorist attack would be devastating. Maritime ports are a vital component of the supply chain, moving the overwhelming majority of cargo into and out of the United States, 99.4 percent by weight, and 64 percent by value, at a value of $3.8 billion each day.

In 2010, the dollar value of cargo that moved the Port of New York and New Jersey alone is more than $175 billion. Anything that threatens this flow of commerce would not only affect the ports themselves, but would also disrupt the supply chain, with widespread effects across the country and around the world.

I might add here, parenthetically, that when I first introduced the legislation, someone said to me that demanding 100 percent scanning might slow the flow of commerce. I replied that one nuclear bomb going off in an American port would eliminate the flow of commerce for a good long time.

Given the very serious nature of the threat we face, I am dismayed that the Department of Homeland Security has not made a realistic effort to implement the 100 percent scanning mandate. Nor has it offered an alternative proposal to achieve the same ends.

I am aware that that Department opposed the original legislation, has never thought that this was a good idea. But it must make a realistic attempt to implement the will of Congress.

I urge DHS to aggressively more forward in implementing the 100 percent maritime cargo scanning mandate. It is one thing to say we cannot achieve this goal this year. It is yet another to declare that the goal itself is not worth pursuing, which unfortunately is something I have heard said.

That would be an enormous mistake. We must continue to take steps toward 100 percent scanning as the ultimate goal. We must not relent in our pursuit of security.

We must not allow gaping holes in our system to go unaddressed. Remember what is at stake here. It seems absurd that we would even entertain the notion that we would perhaps allow a nuclear weapon to be smuggled into our country on board a container that has never been scanned, when we know that if detonated in one of our cities, it would kill millions of people in a deadly flash.

Now it is obvious that the initial statutory deadline this year will not be achieved. However, we can and must make incremental progress that will ultimately get us to the 100 percent standard, while making cargo, our ports and waterways, the American people, more secure in the interim.

We owe the American people no less.

I thank the subcommittee for inviting me to participate in today's hearing. I look forward to continuing to work with my colleagues, the Department of Homeland Security, and other Federal, State, and local agencies, and private stakeholders, on this very important issue.

Mrs. MILLER. Thank you very much, Congressman. We certainly appreciate, again, you taking the time.

We are going to dismiss you and ask for the next panel to come. But I had a chance to talk to you before we started. I recognize certainly your passion on this issue.

That really is going to be the—that was the impetus and will be the crux of all of our questions today, as we can either achieve the mandate of Congress, or if not, as you say, a realistic way to implement, and where we are going with all of this as well.

So it is going to be an interesting hearing.

Mr. NADLER. Thank you very much.

Mrs. MILLER. Thank you.

Mr. CUELLAR. Also, Mr. Nadler, I would say, if Madam Chair——

Mrs. MILLER. Certainly.

Mr. CUELLAR. Just I have no questions, but also I know you worked very hard with Mr. Thompson on this. So I appreciate all the hard work that you put in on this. I appreciate your good work. Thank you.

Mr. NADLER. Thank you, too.

Mrs. MILLER. Thank you.

We all ask the second panel to come forward.

You are all suited up, ready to go here. I think what I will do is just for our panel—and we are looking forward to all your testimony. I will just introduce you all sort of at once. Then we all start with Mr. Heyman.

But let me read your bios a bit here. We are first delighted to have David Heyman, excuse me, assistant secretary for policy at the United States Department of Homeland Security. Previously, he served as the senior fellow and director at the CSIS Homeland Security Program, where he led the research and program activities in homeland security, focusing on developing the strategies and policies to help build and transform the United States' Federal, State, local, and private sector homeland security institutions.

Kevin McAleenan—how do you pronounce it? McAleenan, okay, got it—is the acting assistant commissioner at the Office of Field Operations, Customs and Border Protection. Mr. McAleenan is responsible for overseeing CBP's anti-terrorism, immigration, anti-smuggling, trade compliance, and agricultural protection operations at 20 major field offices, 331 ports of entry, and over 70 locations in over 40 countries internationally, with a staff of more than 28,000 employees and an operating budget of over $3.5 billion.

Rear Admiral Paul Zukunft is the assistant commandant for marine safety, security, and stewardship, and responsible for developing National marine safety, security, and environmental protection doctrine, policy, and regulations, as well as ensuring policy alignment throughout the Federal Government and with international maritime partners.

He recently served as the Federal on-scene coordinator for the Deepwater Horizon incident in the Gulf. We appreciate your service for that horrific incident, and our Nation as well. While there, he directed Federal, State, and local agencies in their response efforts as well.

Mr. Steve Caldwell is the director of maritime security and Coast Guard at the Government Accountability Office, the GAO. His recent reports and testimony covered issues relating to protecting critical infrastructure, the implementation of the Maritime Transportation Security Act and the SAFE Port Act, port security exercises, maritime threat information sharing, maritime domain awareness, container security programs, and risk management for critical maritime infrastructure as well.

The Chairwoman would now recognize Mr. Heyman for his testimony.

STATEMENT OF DAVID HEYMAN, ASSISTANT SECRETARY, OFFICE OF POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. HEYMAN. Thank you, Chairwoman Miller, Ranking Member Cuellar, and other distinguished Members of the subcommittee. Thank you for the opportunity to appear here today.

I am pleased to highlight the Department's work in the area of supply chain security and maritime security. This is an issue of great importance to us.

International trade is this engine that is now the power of economies all around the world. Billions of dollars worth of commodities and merchandises move between trading partners every month by land, sea, and air.

The modern international trading system, or the global supply chain that undergirds the exchange of goods between countries, it is a system that has evolved over decades. We have experienced a dramatic transformation over the past quarter of a century, with the integration and interconnection of buyers and sellers, suppliers and manufacturers all over the world.

Information and communication technologies have enabled this transformation, creating jobs, wealth, and opportunity. Today, that supply chain provides food, medicine, energy, and a myriad of other products that sustain our daily lives.

This is true around the world. It is a model of economic efficiency, enabling just-in-time delivery. But it also means that our economies are more and more interdependent. The expansive nature of the global supply chain system also renders it vulnerable to disruption. We have seen this in terrorist acts, the volcano on Iceland, and in the recent tsunami in Japan.

Disruptions can have a significant impact on our National economies. As such, governments and businesses around the world have a vital interest in transforming the old model of efficiency, and adopting a new model based on ensuring the integrity and reliability of supply chain.

That is precisely what we seek to achieve with the administration's new National Strategy for Global Supply Chain Security; 2 weeks ago, Secretary Napolitano announced the strategy.

It is a strategy to ensure the security and resilience of the global supply chain. It recognizes the critical importance of the system to our economy and security, and lays out an approach to help us foster a transformation from just-in-time to just-in-case.

This country's safety and security will always remain a paramount concern of the Department. The supply chain is an integral component. We have taken a number of significant efforts to strengthen the global supply chain, which we can talk about today.

Specifically on the administration's strategy, it incorporates and builds upon these prior efforts. There are two principle goals: Promoting the timely and efficient flow of legitimate commerce, while protecting and securing the supply chain from exploitation; and No. 2, fostering a global supply chain system that is prepared for and can withstand evolving threats and hazards, and also recover rapidly.

The strategy aligns U.S. and international security and resilience efforts to foster agile systems, able to resolve threats early, improve verification and detection, and reduce vulnerabilities. We do this by galvanating action through a whole-of-Government, all-of-Nation approach, and through managing risk by utilizing layered defenses.

We would like to especially thank the Congress for its foresight, and this committee in particular, in the need for this work, which formed the basis of a strategy under the SAFE Port Act in 2006.

Again, safety and security of the American people is of paramount importance to the Department. The strategy is a significant step forward in this process and evolution.

Over the next 6 months, significant outreach will be conducted to foreign and domestic stakeholders as part of our implementation efforts. This builds on a number of on-going efforts.

In particular, it is worth noting that as a result of Secretary Napolitano's Supply Chain Security Initiative last year, we have already made significant progress implementing the strategy, through new efforts and in some cases new partnerships, such as with the World Customs Organization, the International Maritime Organization, International Civil and Aviation Organization, and the Universal Postal Union.

We are, in fact, helping lead efforts to improve the security of operations across the global supply chain, to raise international standards and foster systems for trade recovery globally.

The written testimony outlines these efforts in greater detail. Let me close with a final thought.

The global supply chain system is an interconnected, multimodal, multi-actor system, highly complex. It encompasses foreign and domestic ports, transportation systems, conveyances, and infrastructure.

Its strength is its ability to deliver goods that sustain our daily lives on a near-real-time basis. That system will continue to grow in scale and importance. So we must recognize today that, without a doubt, disruptions to this system will happen. We must think anew on how to best build in not just efficiency, but security and resilience as well.

Our new National Strategy for Global Chain Security presents a blueprint for change, while building on efforts and infrastructure

that have been in place for some time. We encourage other countries and organizations to adopt similar efforts.

We thank you again for the opportunity to testify, and look forward to answering the questions you may have.

[The joint prepared statement of Mr. Heyman, Mr. McAleenan, and Admiral Zukunft follows:]

JOINT PREPARED STATEMENT OF DAVID HEYMAN, PAUL F. ZUKUNFT, AND KEVIN K. MCALEENAN

FEBRUARY 7, 2012

INTRODUCTION

Chairwoman Miller, Ranking Member Cuellar and other distinguished Members of the subcommittee, thank you for the opportunity to appear before the subcommittee to highlight the Department of Homeland Security's work in the area of supply chain security. This is an issue of singular importance, and we commend the subcommittee for holding this hearing.

International trade is the engine that powers economies all around the world. Billions of dollars worth of commodities and merchandise move between trading partners every month, by land, by sea, and by air. The modern international trading system—or global supply chain—that undergirds the exchange of goods between countries is a system that has evolved over several decades, built incrementally in an effort to reduce costs and expand markets.

We have experienced a dramatic transformation over the past quarter of a century with the extraordinary integration and interconnection of buyers and suppliers and sellers and manufacturers all over the world. The internet and linkages provided by information and communication technologies has helped to enable this transformation. The end result has been the creation of jobs and wealth and opportunity in areas across the globe.

Today, the global supply chain system provides food, medicine, energy, and myriad of other products that support and sustain our daily lives. This is true around the world. It is a model of economic efficiency built to sustain "just-in-time" delivery, but it also means that our economies are more and more interdependent, one upon each other.

However, the expansive nature of the global supply chain system renders it vulnerable to disruption. Disruptions to the global supply chain can be triggered by a range of causes—man-made or naturally occurring—a number of which we have witnessed in recent years. Whether through terrorist acts like the cargo bomb plot in October 2010 or market-driven forces like the slowdown and lockout in 2002 of 29 ports on the West Coast or, most recently, by the volcanic ash clouds of the 2010 eruption of the volcano Eyjafjallajókull in Iceland or the Tsunami that hit Tohoku, Japan in 2011, we see the impact that disruptions can have on our national economies.

Given this, governments and businesses around the world have an interest in transforming the old model of efficiency and adopting a new model based also on ensuring the integrity and reliability of the system as well. In other words, we must move from a model principally focused on "just-in-time" to one also predicated on "just-in-case". It is this notion of a need for greater integrity and reliability that shapes the context for the administration's new—first-ever—strategy to ensure the security and resilience of the global supply chain. It has also been a driving force in our work internationally to foster systems for trade recovery on a global scale.

THE ADMINISTRATION'S NEW NATIONAL STRATEGY FOR GLOBAL SUPPLY CHAIN SECURITY

The United States Government, in collaboration with State, local, Tribal, international, and private sector stakeholders, has undertaken a number of efforts to strengthen the global supply chain. These efforts include implementation of legislative requirements and a number of strategic efforts with a specific security focus. The administration's Strategy incorporates and builds upon those prior efforts.

Initially begun in response to a requirement in the Security and Accountability for Every Port (SAFE Port) Act of 2006 that DHS develop a final *Strategy to Enhance International Supply Chain Security* by July 2010, it was quickly recognized that the multimodal, international nature of the global supply chain system required a broad, all-of-government effort that included input from public and private sector, international, and domestic stakeholders. This effort was led by the National

Security Staff and is intended to inform and guide efforts by all stakeholders, but especially those of the Federal Government.

The focus of the Strategy is the worldwide network of transportation, postal, and shipping pathways, assets, and infrastructure by which goods are moved from the point of manufacture until they reach an end consumer, as well as supporting communications infrastructure and systems. Our approach to supply chain security has two principal goals:

(1) To promote the timely and efficient flow of legitimate commerce, while protecting and securing the supply chain from exploitation and reducing its vulnerabilities to disruption; and

(2) To foster a global supply chain system that is prepared for and can withstand evolving threats and hazards and can recover rapidly from disruptions.

At its core, the Strategy is about a layered, risk-based, and balanced approach in which necessary security measures and resiliency planning are integrated into supply chains. It is about protecting supply chains from being targeted or exploited by those seeking to cause harm. And, it is about maximizing the flow of legitimate commerce. The Strategy achieves this by establishing and adhering to two guiding principles:

(1) Galvanize action through a whole-of-Government, all-of-Nation approach and by collaborating with State and local governments, the private sector and the international community.

(2) Manage risk by utilizing layered defenses, resolving threats as early in the process as possible, and adapting our security posture to changing environments and evolving threats.

Recognizing the good work already accomplished by the United States and the international community, the Strategy does not seek to supplant or impede those efforts. Rather, it seeks to align U.S. and international security and resilience efforts, to foster agile systems able to resolve threats early, improve verification and detection, and reduce systemic vulnerabilities.

The Strategy also sets out eight priority actions upon which immediate implementation efforts will be focused. Through the Strategy, over the next year and beyond, the President has tasked us with:

(1) Aligning Federal activities across the U.S. Government (USG) to the goals of the Strategy;

(2) Refining our understanding of the threats and risks associated with the global supply chain through updated assessments;

(3) Advancing technology research, development, testing, and evaluation efforts aimed at improving our ability to secure cargo in air, land, and sea environments;

(4) Identifying infrastructure projects to serve as models for developing critical infrastructure resiliency best practices;

(5) Seeking opportunities to incorporate global supply chain resiliency goals and objectives into Federal infrastructure investment programs and project assessment processes;

(6) Promoting necessary legislation to support Strategy implementation by Federal departments and agencies;

(7) Developing, in concert with industry and foreign governments, customized solutions to speed the flow of legitimate commerce in specific supply chains that meet designated criteria and can be considered low-risk; and

(8) Aligning trusted trader program requirements across Federal agencies. We will consider the potential for standardized application procedures, enhanced information-sharing agreements, and security audits conducted by joint or cross-designated Federal teams.

The Strategy also fulfills DHS's SAFE Port Act requirement to submit a *Strategy to Enhance International Supply Chain Security,* when combined with the DHS report Fulfilling the SAFE Port Act Requirements, which was transmitted to this committee on January 25, 2012. This SAFE Port Act requirements report addresses those areas of the Act which Congress directed us to consider, such as impacts to small and medium enterprises and supply chain linkages with terrorism financing. As outlined in the report, we considered these issues carefully and they directly informed the development of the goals and objectives of the Strategy.

IMPLEMENTATION OUTREACH TO GLOBAL SUPPLY CHAIN STAKEHOLDERS

Recognizing the interconnected nature of the global supply chain system, the Strategy emphasizes that continued collaboration with global stakeholders is critical.

Over the 6 months following its release, significant outreach will be conducted by the United States to foreign and domestic stakeholders. We are soliciting their views on how best to implement the Strategy and how best to foster a secure, efficient, and resilient global system.

Outreach to our foreign partners will be accomplished through a collaborative process in which the Department of State and DHS engage with appropriate government Ministries and organizations. This engagement will educate our partners on our strategic goals and objectives and solicit their input of how we can best implement secure, efficient, and resilient systems that span the globe, from the beginnings of supply chains to their end.

We will confer with our domestic partners through a Cross Sector Supply Chain Working Group that DHS has established under the Critical Infrastructure Partnership Advisory Council. Through this process, Critical Infrastructure Sectors will be consulted through their Sector Coordinating Councils (SCC). The general public, or industry segments that do not directly participate in the SCCs, will be able to participate in these discussions as subject matter experts, ensuring we obtain the broadest possible input.

We are specifically interested in receiving views and recommendations from governments, transportation sector partners, and other affected stakeholders on, but not limited to, the following areas:

- Specific opportunities to implement the goals of the Strategy and enhance the security, efficiency, and resilience of the global supply chain;
- Understanding evolving threats (man-made as well as natural) and vulnerabilities in the global supply chain as a whole and among different modes of transportation;
- Opportunities to develop or advance international best practices, standards, or guidelines for reducing threats/vulnerabilities and opportunities to encourage global implementation of them;
- Opportunities for the USG to work in concert with industry and the international community to further strengthen the global supply chain, including ways to increase participation in and improve the cost-effectiveness of private-public partnership programs;
- Assumptions that currently inform supply chain security policies and programs that may be incorrect, dated, or obsolete.

The results of the outreach will be combined with other, on-going work, including threat and risk assessments, to support Federal department and agency implementation planning.

BUILDING ON PAST AND ON-GOING INITIATIVES

- While the *National Strategy for Global Supply Chain Security* speaks to our future focus, we would like to address current efforts to secure our ports and waterways and collaborate with our international partners.

Global Initiatives

As discussed previously, we recognized early in the Strategy development process that supply chains are inherently interconnected, intermodal—and global. Even as the Strategy was being created, DHS increased its emphasis on working with the international community to enhance efficiency, security, and resilience and meet the President's strategic goals. Our on-going efforts now that the Strategy has been released will form a basis for our implementation activities.

In January, 2011, Secretary Napolitano identified global supply chain security as a focal point for our Department.

She specifically emphasized the need for global collaboration—and met with the Secretary Generals of the International Maritime Organization (IMO), the International Civil Aviation Organization (ICAO), and the World Customs Organization (WCO), as well as the leadership of the Universal Postal Union (UPU).

Her engagement has resulted in seven international objectives, which we have been actively pursuing:

(1) Identifying and Responding to Evolving Threats/Risks;
(2) Expanding Advance Information Requirements Across All Modes;
(3) Streamlining "Trusted Trader" Programs;
(4) Stemming the Flow of Illicit Shipments of Dangerous Materials;
(5) Securing and Facilitating Air Cargo and Global Mail;
(6) Building a Resilient System; and
(7) Exploring and Deploying New Technologies.

There has been significant progress since January 2011, including not only the practical efforts to improve the security of operations across the global supply chain, but also advancing the institutionalization of these efforts on an international level

through new work streams, international bodies committed to our objectives, and new standard-setting processes. Among other results, our work with our partners has had the following impacts:

- The WCO has developed a Risk Management Compendium, enabling Customs administrations to operate under common terminology and criteria to target both high- and low-risk cargo.
- The ICAO is currently finalizing its Risk Context Statement, which will be presented to the Aviation Security Panel of Experts in March, 2012, creating a common risk definition for aviation security.
- The ICAO established a Transshipment sub-working group to address air cargo that is transshipped through world airports.
- The IMO has completed a user's guide for *International Ship and Port Facility Security (ISPS) Code* implementation, enhancing compliance and understanding of port security standards.
- The WCO has revised its advance data guidelines, modeled after DHS's Importer Security Filing rule (better known as "10+2") and is working on refining air cargo advance data guidelines in coordination with the Air Cargo Advance Screening pilots currently being conducted by DHS.
- DHS has been actively aligning "trusted trader" programs such as the Customs Trade Partnership Against Terrorism (C–TPAT) and the "trusted shipper" concept, and are working with the ICAO and WCO toward creating common global standards.
- The Immigration and Customs Enforcement (ICE) project Global Shield has transitioned into the WCO Program Global Shield, with significantly expanded—and growing—participation across the globe to detect illegal activity and mitigate the misdirection of improvised explosive device precursor materials through seizures and arrests. Under Program Global Shield, more than 89 participating countries are currently sharing information with each other to ensure that chemicals entering their countries are being used in safe and legal ways. As of December 2011, Program Global Shield has accounted for seizures of chemical precursors totaling over 45 metric tons and 19 arrests related to the illicit diversion of these chemicals.
- The International Atomic Energy Agency (IAEA), in collaboration with DNDO, is developing technical standards for detection devices and recommendations on addressing nuclear and other radioactive materials out of regulatory control. DHS is also working with the IAEA to establish an Action Plan to finalize a list of detection technologies that meet international standards by April 2012. Based on their analysis, shortfalls in current standards will be identified and targeted for action.
- Work is on-going with the UPU to strengthen advance information for mail and postal operations and develop a strategy embracing security and advance data sharing measures for consideration at the UPU Congress in October 2012. The UPU has established emergency contacts in all countries to facilitate the adjudication of potential security alerts and is establishing an international standard for the handling and resolution of anomalies detected at international mail transit hubs.
- The Asia-Pacific Economic Cooperation (APEC) adopted regional information guidelines for government-to-government and government-to-private sector communications related to trade recovery in September, 2011. The APEC information guidelines were subsequently adopted by the WCO, creating global guidelines, in December, 2011.

Bilateral Agreements and Partnerships

Specific to supply chain security, DHS has entered into Joint Statements or publicly affirmed our mutual commitment through published meeting summaries and statements with a number of nations, and is discussing additional statements with key partners. These statements reaffirm our commitment and our partners' commitments to cooperate, identify key areas of mutual emphasis and principles, and encourage collaboration in our efforts with multilateral forums such as the IMO, ICAO, and WCO. To date, Joint Statements have been signed with New Zealand and the European Commission, and supply chain security has been specifically addressed with the Russian Federation, India, and Canada.

To increase the operational reach of U.S. assets, and to enable partner nation assets to patrol and respond to threats in their own sovereign waters, the U.S. Government has entered into 41 bilateral maritime counter-drug law enforcement agreements. Additionally, the Coast Guard has developed non-binding operational procedures with Mexico, Ecuador, and Peru to facilitate communications between operation centers for the confirmation of registry requests and for permission to

stop, board, and search vessels. Coast Guard law enforcement and border security capabilities are evident at both the National and the port level.

The Strategy, and our international agreements and partnerships, also directly support the President's priorities as outlined in the "Beyond the Border" Initiative with Canada and the "21st Century Border Management" Agreement with Mexico. Indeed, many of the specific activities associated with the efforts were informed by and aligned with the strategy during their development.

International Port Security

To address threats farthest from our borders, the Coast Guard establishes and fosters strategic relationships with other nations and international forums. The ISPS Code was created by the IMO with significant Coast Guard assistance. The ISPS Code provides an international regime to ensure ship and port facilities take appropriate preventive measures to ensure security, similar to our domestic regime in the Maritime Transportation Security Act. The International Port Security (IPS) Program sends Coast Guard men and women to foreign ports that conduct maritime trade with the United States to assess the effectiveness of their antiterrorism measures and to verify compliance with ISPS Code. To date, the IPS Program has assessed more than 900 ports and facilities in more than 150 countries.

In 2011, the IPS program assessed the effectiveness of 211 port facilities in 76 of our maritime trading partners. Two countries were found to not have adequate anti-terrorism measures in place in their ports. As a result, they were added to the Coast Guard's Port Security Advisory (PSA) and conditions of entry (COE) were imposed on vessels that have visited one of those ports during their last several port calls before arriving in the United States.

The Coast Guard also supports the European Commission, the Organization of American States, the APEC, and the Secretariat of the Pacific Community to reduce the number of non-compliant foreign ports, thereby reducing and mitigating risk to U.S. ports. Vessels arriving to the United States from non-ISPS compliant countries are required to take additional security precautions, may be boarded by the Coast Guard before being granted permission to enter, and may be refused entry.

As a result of the enactment of the Coast Guard Authorization Act of 2010, the Coast Guard received additional authority to conduct capacity-building activities. The Coast Guard has implemented a Port Security Engagement Strategy to expand its engagement with countries beyond minimal ISPS Code implementation to a more robust effort to improve all aspects of port security including legal regimes, maritime domain awareness, and port security operations. The Coast Guard has also developed a Return on Investment Model that identifies countries where capacity-building activities would be of the most benefit.

Finally, DHS is pursuing a "Mutual Recognition" Memorandum of Understanding (MOU) with the European Commission (EC). The MOU would call for mutual joint inspections of each other's ports, and the Coast Guard would recognize a successful EC inspection of its Member State's ports the same as a successful country visit by the IPS Program. A similar arrangement is being contemplated with Canada.

Maritime Domain Awareness and Offshore Operations

Maritime Domain Awareness (MDA) is a diverse set of capabilities that support all levels (strategic, operational, and tactical) of decision-making. MDA is more than an awareness of ships en route to a particular port; it also entails knowledge of:

- People: Crew, passengers, owners, and operators;
- Cargo: All elements of the global supply chain;
- Infrastructure: Vital elements of the Nation's maritime infrastructure, including facilities, services, and systems;
- Environment: Weather, environmentally sensitive areas, and living marine resources; and
- Trends: Shipping routes, migration routes, and seasonal changes.

Effective MDA requires efficient information sharing that demands coordination among numerous participants at international, Federal, regional, State, local, territorial, and Tribal levels of government, as well as with maritime industry and private sector partners.

The Coast Guard's major cutters and deployable forces are critical to the layered security approach. The Coast Guard's mix of cutters, aircraft, and boats—all operated by highly proficient personnel—allow the Coast Guard to maximize its unique authorities to exercise layered and effective security.

Maritime Intelligence and Targeting

As the lead DHS agency for maritime homeland security, the Coast Guard screens ships, crews, and passengers for all vessels required to submit a 96-hour Notice of Arrival (NOA) to a U.S. port. CBP's National Targeting Center (NTC), supported by

Coast Guard staff, vets passengers, personnel, and cargo destined for the United States. Further vetting of the NOA is performed by the Intelligence Coordination Center (ICC), while the two Maritime Intelligence Fusion Centers (MIFCs) focus on screening the vessel itself. The MIFCs associate relevant intelligence and law enforcement analysis to specific vessels, and assess vessel activity. Screening results are passed to the appropriate Coast Guard Sector Command Center, local intelligence staffs, and CBP field offices to be used to ascertain the potential risk posed by a vessel.

At Home In Our Ports

Coast Guard Captains of the Port (COTP) are designated as the Federal Maritime Security Coordinator for their port. In this role they lead the Area Maritime Security (AMS) Committees, which often include representatives from CBP, ICE, and the TSA, and oversee the development and regular review of the AMS Plans. AMS Committees have developed strong working relationships with other Federal, State, Tribal, territorial, and local law enforcement agencies in an environment that fosters maritime stakeholder participation. Each AMSC reflects the unique challenges and environment of the local port community.

On a National scale, the establishment of Interagency Operations Centers (IOCs) for port security is well under way. Coast Guard, CBP, and other agencies are sharing workspace and coordinating operational efforts for improved efficiency and effectiveness of maritime assets in ports including Charleston, Puget Sound, San Diego, Boston, and Jacksonville.

The Coast Guard is also responsible for inspecting U.S. port facilities and vessels for safety and security and ensuring compliance with U.S. laws and regulations. In 2011, 10,209 facility safety and security inspections were completed and more than 9,500 Port State Control and Security examinations were conducted on foreign-flag vessels.

Cargo Security and Supply Chain Integrity

As the lead DHS agency for cargo security, CBP is at the front line of protecting the Nation from threats, including those posed by containerized cargo. CBP's security and trade facilitation missions are mutually supportive: By utilizing risk-based strategies, and applying a multilayered approach, CBP can focus time and resources on the small percentage of goods that are high-risk or about which we know the least, which in turn allows CBP to expedite trade that is low-risk or about which we already know a great deal. This approach improves supply chain integrity, promotes economic viability and increases resilience in the event of a disruption to the global supply chain.

CBP's multilayered security approach involves:

- Obtaining information about cargo and those involved in moving it early in the process;
- Using advanced targeting techniques to assess risk and build a knowledge base about the people and companies involved in the supply chain;
- Fostering partnerships with the private sector and collaborating with other Federal agencies and departments, such as the U.S. Coast Guard, Department of Health and Human Services, the Consumer Product Safety Commission, ICE, and the Department of Agriculture, and with foreign governments, including through information sharing;
- Expanding enforcement efforts to points earlier in the supply chain than simply at our borders; and
- Maintaining robust inspection regimes, including non-intrusive inspection equipment and radiation detection technologies, at our ports of entry.

CBP requires advance electronic cargo information, as mandated in the Trade Act of 2002 (24-Hour Rule, through regulations), for all in-bound shipments in all modes of transportation. CBP requires the electronic transmission of additional data, as mandated by the SAFE Port Act, through the Importer Security Filing and Additional Carrier Requirements rule (Security Filing "10+2"), which became effective as an Interim Final Rule on January 26, 2009, and went into full effect on January 26, 2010. Security Filing "10+2" joins the 24-hour rule, and the C–TPAT program and Container Security Initiative (CSI) discussed below, in collecting advance information to improve CBP's targeting efforts.

As part of CBP's layered targeting strategy, the National Targeting Center—Cargo (NTC–C) proactively analyzes advance cargo tactical and strategic information using the Automated Targeting System (ATS) before shipments reach the United States. ATS 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 targeting rules, the ATS

alerts the user to data that meets or exceeds certain predefined criteria. National targeting rule sets have been implemented in ATS to provide threshold targeting for National security risks for all modes of transportation—sea, truck, rail, and air. ATS is a decision support tool for CBP officers working in the NTC–C and in Advanced Targeting Units at our ports of entry and CSI ports abroad allowing officers to focus on the highest threats while facilitating legitimate trade.

NTC–C has established partnerships and liaisons with other agencies, both domestically and abroad. Partnerships with ICE, the Drug Enforcement Administration, the Financial Crimes Enforcement Network (FinCEN), the Department of Commerce, and the Department of Health and Human Services 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.

Customs Trade Partnership Against Terrorism (C–TPAT)

CBP works with the trade community through the C–TPAT, a voluntary public-private partnership program wherein some members of the trade community adopt tighter security measures throughout their international supply chain and in return are afforded benefits such as reduced exams, front-of-line examination privileges to the extent possible and practical, and an assigned Supply Chain Security Specialist who helps them maintain compliance. C–TPAT has enabled CBP to leverage private sector resources to enhance supply chain security and integrity.

CBP conducts records checks on the company in its law enforcement and trade databases and ensures the company meets the security criteria for its particular business sector. Members who pass extensive vetting are certified into the program. Using a risk-based approach, CBP Supply Chain Security Specialists conduct on-site visits of foreign and domestic facilities to confirm that the security practices are in place and operational.

C–TPAT has been a success—membership in this program has grown from 7 companies in its first year to 10,221 as of January 12, 2012. Additionally, CBP is working with foreign partners to establish bi-national recognition and enforcement of C–TPAT. CBP currently has signed mutual recognition arrangements with New Zealand, Canada, Jordan, Japan, and Korea and is continuing to work towards similar recognition with the European Union, Singapore, Taiwan, and other countries.

Container Security Initiative (CSI)

Close coordination and joint operations with CBP and ICE in international programs are also critical. The CSI 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.

Through CSI, CBP stations multidisciplinary teams of officers to work with host country counterparts to identify and examine containers that are determined to pose a high risk for terrorist activity. CSI, the first program of its kind, was announced in January 2002 and is currently operational in 58 foreign seaports—covering more than 80 percent of the maritime containerized cargo shipped to the United States.

CBP officers stationed at CSI ports, with assistance from CSI targeters at the NTC–C, review 100 percent of the manifests originating and/or transiting those foreign ports for containers that are destined for the United States. In this way, CBP identifies and examines high-risk containerized maritime cargo prior to lading at a foreign port and before shipment to the United States. In fiscal year 2011, CBP officers stationed at CSI ports reviewed over 9.5 million bills of lading and conducted 45,500 exams in conjunction with their host country counterparts.

CBP is exploring opportunities to utilize emerging technology in some locations, which will allow the program to become more efficient and less costly. In January 2009, CBP began to reduce the number of personnel stationed overseas who perform targeting functions, increasingly shifting more of the targeting of high-risk containers to personnel stationed at the NTC–C. This shift in operations reduces costs without diminishing the effectiveness of the CSI program. CSI will become a hybrid of different operational protocols designed around the uniqueness of each foreign port. CBP will remain operational in all 58 locations in fiscal year 2012 with sufficient personnel in country to conduct the examinations of high-risk shipments with the host government and to maintain relationships with their host-country counterparts.

Secure Freight Initiative (SFI)

The SFI partnered with the Department of Energy deploying networks of radiation detection and imaging equipment at six overseas pilot ports. All pilot operations, with the exception of Qasim, Pakistan have ended and those ports have re-

verted back to the CSI protocols of risk-based targeting. The pilots encountered a number of serious challenges to implementing the 100% scanning mandate.

While each port presented a unique set of challenges, most of the challenges were universal in nature. CBP has documented numerous challenges associated with implementing 100 percent scanning including diplomatic challenges, international trade opposition, the need for port reconfiguration, potential for reciprocal requirements on the United States and lack of available technology to efficiently scan transshipped cargo. It is also important to keep in mind that approximately 80% of the cargo shipped to the United States is sent from only 58 of more than 700 ports. Installing equipment and placing personnel at all of these ports—regardless of volume—would strain Government resources without a guarantee of results.

Non-Intrusive Inspection (NII)/Radiation Detection Technology

The deployment of imaging systems and radiation detection equipment has made a tremendous contribution to CBP's progress in securing the supply chains that bring goods into the United States from around the world against exploitation by terrorist groups. NII technology serves as a force multiplier that allows officers to detect possible anomalies between the contents of a container and the manifest. CBP's use of NII allows us to work smarter and more efficiently in recognizing potential threats and allows cargo to move more expeditiously from the port of entry to the final destination.

CBP has aggressively deployed NII and Radiation Portal Monitor (RPM) technology. Prior to 9/11, only 64 large-scale NII systems, and not a single RPM, were deployed to our country's borders. Today CBP has 301 NII systems and 1,388 RPMs. To date, CBP has used the deployed NII systems to conduct over 60 million examinations, resulting in over 11,200 narcotic seizures, with a total weight of over 3.2 million pounds, and more than $45.9 million in undeclared currency seizures. CBP uses RPMs to scan 99 percent of all in-coming containerized cargo arriving in the United States by sea and 100% of all passenger and cargo vehicles entering the U.S. land ports of entry. Since RPM program inception in 2002, CBP has scanned over 679 million conveyances for radiological contraband, resulting in more than 2.8 million alarms. CBP's Laboratories and Scientific Services 24/7 Teleforensic Center spectroscopy group at the NTC has responded to nearly 53,000 requests from the field for technical assistance in resolving alarms. To date, 100 percent of alarms have been successfully adjudicated as legitimate trade.

CONCLUSION

The global supply chain system is an interconnected multimodal system, encompassing foreign and domestic ports, transportation systems, conveyances, and infrastructure. Enhancing its security, efficiency, and resilience requires a culture of mutual interest and shared responsibility among stakeholders throughout the world. It requires a balanced approach and the dedication of resources, collaboration—and where necessary, compliance verification and enforcement.

While our efforts to date have been successful, we recognize that further diligence is required. Our new *National Strategy for Global Supply Chain Security* presents a blueprint for change, while building on efforts and infrastructure that have been in place for some time. The risk of natural disasters and other disruptions to the global supply chain presents a risk to our Nation's economic strength and vitality. Our Strategy presents an opportunity to continue to promote America's future economic growth and international competitiveness by remaining open and thriving for business.

Thank you again for this opportunity to testify about our efforts.

We look forward to answering any questions you may have.

Mrs. MILLER. Thank you very much. Appreciate that testimony.

The Chairwoman now recognizes Mr. McAleenan for his testimony.

STATEMENT OF KEVIN MCALEENAN, ACTING ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MCALEENAN. Madam Chairwoman, Ranking Member Cuellar, esteemed Members of the subcommittee, it is a privilege and honor to appear before you today to discuss U.S. Customs and

Border Protection's work to balance maritime security and trade facilitation, protecting the country from dangerous shipments, and enhancing the security of the global supply chain, while expediting legitimate commerce.

Customs and Border Protection, or CBP, is charged with managing the physical access to our economy and our Nation and ports of entry. At the core of that responsibility, we are on the front lines of protecting our Nation from threats, including those that could potentially be introduced in cargo shipments.

Just as importantly, CBP is on the front lines of protecting our economic future by facilitating legitimate trade through our ports. Through the use of better information, technology, partnerships, we have been able to form the most effective supply chain security structure in the world, helping to reduce transaction costs for U.S. business, and provide an environment where U.S. security and business interests can work together toward our common mission.

To meet our responsibilities, we have worked to identify and address potential threats before they arrive at our ports. This requires that we secure the flow of cargo at each stage of the supply chain, the point of origin, while in transit, and when it arrives in the United States.

To accomplish this, CBP pursues a multi-layered approach to security, segmenting cargo by potential risk, and examining it as early as possible in the process. Although often presented as being in tension or conflict, our security and trade facilitation missions are mutually supporting.

By utilizing a risk-based strategy, we can focus our time and resources on the small percentage of goods that are higher risk, which in turn allows us to expedite trade that is low risk or about which we already know a great deal.

Our multi-layered approach is based on the following core elements: Obtaining information about cargo shipments as early in the process as possible, using sophisticated targeting techniques to assess each shipment for risk, partnering with the private sector to secure supply chains from the manufacturer to the importer, working with foreign governments and international organizations like the World Customs Organization to harmonize and enhance approaches to supply chain security, and maintaining a robust inspection regime, including non-intrusive inspection equipment and radiation detection technology at our ports of entry.

I am sure these elements are quite familiar to the subcommittee, especially in light of how these tenets are fundamental to the approach taken in the new National strategy.

Over the past several years, DHS and CBP, often working closely with you and your staff, have achieved significant advances on both cargo security and trade facilitation. Allow me to highlight a few.

With your support, we have implemented the Import Security Filing, of 10+2. Building on the 24-hour rule, this program provides additional insight into the supply chain, allowing us to identify potential risks more accurately, and allowing our trade partners to identify inefficiencies in their processes.

We have developed and enhanced the unique capabilities of the National Targeting Center for Cargo to proactively analyze advanced cargo information using the automated targeting system,

which allows us to take action before shipments are loaded onto vessels and aircraft destined to the United States.

The CBP Trusted Shipper Program, the Customs Trade Partnership Against Terrorism, or C–TPAT, has long been recognized as the model for true collaboration between Government and business. Today, there are over 10,000 members, representing over 55 percent of the imported value into this country.

While terrorism will remain the primary C–TPAT focus, we will explore ways to collaboratively address other threats that have the potential to compromise the supply chain, including drug smuggling, weapons trafficking, and trade and import safety violations.

Under the Container Security Initiative, or CSI, CBP continues to work with our international partners to mitigate the threat that high-risk maritime cargo present before it leaves the foreign ports. Today, CBP CSI maintains operations at 58 ports in 32 countries, screening approximately 80 percent of the maritime cargo being shipped to the United States.

We are continuing our aggressive deployment and use of advance imaging systems and radiation detection equipment at our ports. This non-intrusive inspection technology allows us to work smarter and more efficiently in recognizing potential threats.

These highlights demonstrate that CBP remains at the forefront of supply chain management. I am confident that the approach laid out in the National strategy represents an effective way forward, building on these existing programs.

Thank you again for the opportunity to testify about CBP's commitment to enhancing cargo security and trade resilience.

We look forward to continuing to work with the subcommittee on these issues. I will be happy to take any of your questions.

Mrs. MILLER. Thank you very much.

The Chairwoman now recognizes Admiral Zukunft.

STATEMENT OF REAR ADMIRAL PAUL ZUKUNFT, ASSISTANT COMMANDANT FOR MARINE SAFETY, SECURITY, AND STEWARDSHIP, U.S. COAST GUARD, U.S. DEPARTMENT OF HOMELAND SECURITY

Admiral ZUKUNFT. Good morning, Chairwoman Miller, Ranking Member Cuellar, and distinguished Members of the subcommittee.

I am honored to appear before you today to speak about the Coast Guard's layered approach to protecting our ports, maritime commerce, and securing the global maritime supply chain.

From our inception, the United States has been a maritime Nation. Considering that high concentrations of our population live and around port areas, and 95 percent of our international trade is done via the sea, the consequences of any attack or disruption on our maritime transportation system are potentially severe.

Backed by the Maritime Transportation Security Act of 2002, and the Security and Accountability for Every Port Act of 2006, the Coast Guard has led a joint Federal, State, local, Tribal, private sector, and international charge to implement a robust, layered security approach, that starts in ports abroad, carries across the high seas, and culminates in our domestic waterways, designed to identify and stop any threat long before it reaches our shores.

Our efforts start abroad under the auspices of the International Ship and Port Facility Security Code, which guides the Coast Guard's overseas assessment at more than 900 port facilities and 153 of the 157 countries that could potentially conduct maritime commerce with the United States.

For example, in 2010, two companies commenced the shipment of liquefied natural gas from Yemen to the United States. Due to the increased terrorist risk at the origin, the Coast Guard conducted additional port assessments in Yemen, and are now using biometric technologies to screen arriving crew members before they depart Yemen.

Those vessels are also inspected with an undersea inspection, well in advance, in the Mediterranean Sea, before they make arrival in U.S. ports.

Offshore, a major cutter fleet maintains a vigilant presence, conducting fisheries enforcement, counter-drug, alien migrant interdiction operations, while armed with the authorities of 41 bilateral agreements, and simultaneously maintaining an agile posture to respond to humanitarian disasters and threats to maritime security and the global supply chain.

The Coast Guard's planned fleet of National Security Cutters and Offshore Patrol Cutters, augmented by our long-range C–130s, maritime patrol craft, and working with Customs and Border Patrol, are essential to maintaining this offshore response capabilities.

Additionally, the Coast Guard, in cooperation with U.S. Customs and Border Protection, ensure that U.S.-bound vessels that pose a potential risk are identified and inspected before they reach U.S. shores. Specifically, the Coast Guard and CBP share and jointly screen manifests 96 hours prior to a vessel's arrival in the United States, to identify crew, cargo, vessel documentation, and route anomalies, thereby providing an appropriate lead time to marshal a response to any threat well off-shore.

In 2011, the Coast Watch Program, run by Coast Guard's Intelligence Coordination Center, screened 28.5 million people and more than 121,000 ship arrivals, as well as their business practices and associations, and generated 120 advanced warnings on arriving ships, cargoes, and persons posing a potential security or criminal threat.

The Coast Guard leads the International Maritime Organization's Workgroup Three, which focuses on combating piracy on the high seas. This effort has resulted in several best practices, such as the use of private armed security teams on-board commercial vessels transiting the high-risk waters.

In 2011, these teams repelled over 120 attacks that would have otherwise impacted the global supply chain.

Our final level of security resides in our domestic ports and waterways. Since 2004, we have reviewed, approved, and verified compliance of security plans for more than 11,000 U.S. vessels, 3,200 domestic port facilities, and through the use of area maritime security committees, have fostered an extensive interagency collaboration to bolster the security of our critical infrastructure.

This layered maritime security approach was highlighted in 2010 when the motor vessel Sun Sea, carrying almost 500 illegal mi-

grant smugglers, with ties to the Tamil Tigers from Sri Lanka, to Canada, was intercepted by Canadian forces who were supported by Coast Guard operational intelligence resources.

This case demonstrated our capacity and capability to track and intercept a potential threat on the high seas, and mitigate risk to our homeland. It was also a prime utilization of our Maritime Operational Threat Response Plan, a Presidential-directed interagency process that establishes protocols for real-time communication, coordination, and decisionmaking among interagency principals.

Thank you for the opportunity to appear before you today, and for your continued support of the Coast Guard. I will be pleased to answer your questions.

Mrs. MILLER. Thank you very much, admiral.

The Chairwoman now recognizes Mr. Caldwell for his testimony.

STATEMENT OF STEPHEN L. CALDWELL, DIRECTOR, MARITIME AND COAST GUARD ISSUES, HOMELAND SECURITY AND JUSTICE TEAM, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. CALDWELL. Chairman Miller, Ranking Member Cuellar, and other Members of the committee, thank you very much for having GAO up here to talk about supply chain security.

I think it is important to recognize that the issues and programs that we are talking about today didn't start with the Secretary's or the President's Strategy from last week. These things go back 10 years.

They go back to 9/11. They go back to the Maritime Transportation Security Act, which was passed in November about 10 years ago.

The Maritime Transportation Security Act, among other things, called for a secure system of international intermodal transportation, including standards and procedures for screening, evaluating, and monitoring cargo while in transit.

Since 9/11, GAO has conducted about two dozen reports on some aspects of supply chain security, everything from the programs that have been discussed to a lot of the technologies that have been used, some successfully, and some attempts that haven't been as successful.

Many of these programs were jump-started right after 9/11. So I think it was important to understand some of the—that they had initially. GAO made a number of recommendations through the years for DHS to improve its strategic planning, workforce management, internal controls, cost estimates, and performance measures.

As these programs developed, a lot of GAO's recommendations were implemented. Through that and the maturation of the programs, they have certainly improved over the years.

I will be happy to discuss any of those individual programs during the Q&A session.

Now regarding the 100 percent scanning, the new strategy itself does not mention the existing statutory requirement. We completed a thorough review of the 100 percent scanning back in 2009. We cited a number of challenges which did bring into question the feasibility of whether we can do that as called for in the law.

In our report, we made a number of recommendations. For example, we recommended that DHS develop more accurate cost estimates of what it might cost, conduct a cost/benefit analysis, conduct a formal feasibility analysis, and after doing all of these, provide specific alternatives to Congress, including potential legislation.

Unfortunately, and despite the issuance of the recent strategy, really little has changed in terms of our recommendations in the last 2 or 3 years. While DHS partially concurred with our recommendations at that time, they haven't implemented most of those.

They now indicate that these recommendations are largely overcome by events. We think that if DHS had implemented these recommendations a while back, the Department would be in a much stronger position to talk about what those alternatives should be to 100 percent scanning, and actually have specific legislative things.

It would also be in a stronger position to justify the waivers that the Department will obviously have to be providing and notifying Congress about relatively soon. In fact, I think if these recommendations had been implemented 2 to 3 years ago, we might already have some kind of maybe legislated compromise and be quite a bit ahead from where we are right now.

So here we are. We are still at kind of an impasse in turns of the legislative requirement of the 100 percent scanning. Our industry and trade partners are still very concerned about the uncertainty this creates for them.

This is both our domestic industry as well as international industry.

DHS will soon have to implement their chosen path in terms of doing a blanket waiver for all ports, and provide Congress with advanced notification of that. There are substantial reporting requirements to that waiver. Those will continue as long as DHS uses the waivers as their preferred tool to meet the requirements of denial of an act.

In closing, GAO stands ready to continue providing analysis to Congress on these issues. I thank you. I will be happy to answer questions along with the rest of the panel.

[The statement of Mr. Caldwell follows:]

PREPARED STATEMENT OF STEPHEN L. CALDWELL

FEBRUARY 7, 2012

GAO HIGHLIGHTS

Highlights of GAO–12–422T, a testimony before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

Cargo containers that are part of the global supply chain—the flow of goods from manufacturers to retailers—are vulnerable to threats from terrorists. The Maritime Transportation Security Act (MTSA) of 2002 and the Security and Accountability For Every (SAFE) Port Act of 2006 required the Department of Homeland Security (DHS) to take actions to improve maritime transportation security. Also, 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 all U.S.-bound cargo containers be scanned. Within DHS, U.S. Customs and Border Protection (CBP) is responsible for container security programs to address these requirements. This testi-

mony addresses, among other things: (1) Efforts to gather advance information about container shipments to assess risks, (2) technologies used to protect the integrity of containers and scan them, and (3) the status of efforts to scan 100 percent of U.S.-bound containers. GAO's statement is based on products issued from April 2005 through July 2011, along with selected updates conducted from January to February 2012. Updates involved collecting information from CBP on the status of efforts to address GAO's prior recommendations on these issues and its plans to implement 100 percent scanning.

What GAO Recommends

GAO has made recommendations in past reports to DHS to strengthen its container security efforts. DHS concurred with GAO's recommendations and has either addressed them or is undertaking efforts to address them.

SUPPLY CHAIN SECURITY.—CONTAINER SECURITY PROGRAMS HAVE MATURED, BUT UNCERTAINTY PERSISTS OVER THE FUTURE OF 100 PERCENT SCANNING

What GAO Found

As part of its efforts to identify high-risk cargo for inspection, CBP uses various sources of information to screen containers in advance of their arrival in the United States. For example, in 2009, CBP implemented the Importer Security Filing and Additional Carrier Requirements to collect additional information for targeting. The additional cargo information required, such as country of origin, is to be provided to CBP in advance of arrival of the cargo containers at U.S. ports. In September 2010, GAO recommended that CBP establish milestones and time frames for updating its targeting criteria to include the additional information. In response, CBP updated its targeting criteria in January 2011.

DHS has made some progress in developing and implementing container security technologies to protect the integrity of containers and to scan them. GAO reported in September 2010 that DHS's Science and Technology Directorate initiated four container security technology projects to detect and report intrusions into cargo containers. However, operational testing had not occurred to ensure the prototypes would function as intended. Therefore, GAO recommended that testing and evaluation occur in all environments in which DHS planned to implement the technologies. DHS concurred and has made progress implementing this recommendation. To prevent the smuggling of nuclear and radiological materials, CBP, in coordination with the Domestic Nuclear Detection Office (DNDO), has deployed over 1,400 radiation portal monitors (RPM) at U.S. ports of entry to detect the presence of radiation in cargo containers. Since 2006, GAO reported on problems with DNDO's efforts to deploy a more advanced and significantly more expensive type of RPM. Among other things, GAO reported that an updated cost-benefit analysis might show that DNDO's program to replace existing equipment with the advanced technology was not justified. After spending more than $200 million, DHS ended the program in July 2011.

Uncertainty persists over how DHS and CBP will fulfill the mandate for 100 percent scanning given that the feasibility remains unproven in light of the challenges CBP has faced implementing a pilot program for 100 percent scanning. In response to the SAFE Port Act requirement to implement a pilot program to determine the feasibility of 100 percent scanning, CBP, the Department of State, and the Department of Energy announced the formation of the Secure Freight Initiative (SFI) pilot program in December 2006. However, logistical, technological, and other challenges prevented the participating ports from achieving 100 percent scanning and CBP has since reduced the scope of the SFI program from six ports to one. In October 2009, GAO recommended that CBP perform an assessment to determine if 100 percent scanning is feasible, and if it is, the best way to achieve it, or if it is not feasible, present acceptable alternatives. However, to date, CBP has not conducted such an assessment or identified alternatives to 100 percent scanning. Further, as GAO previously reported, DHS acknowledged it will not be able to meet the 9/11 Act's July 2012 deadline for implementing the 100 percent scanning requirement, and therefore, it expects to grant a blanket extension to all foreign ports pursuant to the statute, thus extending the target date to July 2014. To do so, DHS is required to report to Congress by May 2, 2012, of any extensions it plans to grant.

Chairman Miller, Ranking Member Cuellar, and Members of the subcommittee: I am pleased to be here today to discuss the status of Federal efforts to enhance the security of maritime cargo containers used for shipping many imports to the United States. The potential for terrorists to smuggle weapons of mass destruction (WMD) inside cargo containers bound for the United States has remained a concern since the terrorist attacks of September 11, 2001. Cargo containers are an important

segment of the global supply chain—the flow of goods from manufacturers to retailers. In 2011, about 10.7 million ocean-borne cargo containers arrived at U.S. ports, and according to the U.S. Department of Transportation, the majority of U.S. imports arrive by ocean vessel.[1] The typical supply chain process for transporting cargo containers to the United States involves many steps and participants. For example, the cargo containers, and the goods in them, can be compromised not only by the manufacturers or suppliers of the goods being shipped, but also by vessel carriers who are responsible for transporting the containers from foreign ports to U.S. ports, as well as by personnel who load and unload cargo containers onto and off vessels.[2]

Given the complexity of the global supply chain process and the vast number of cargo containers that are shipped to the United States each year, the global supply chain is vulnerable to threats that terrorists and criminals might be able to exploit. As we reported in October 2009, while the Department of Homeland Security (DHS) has noted that the likelihood of terrorists smuggling WMD into the United States in cargo containers is low, the Nation's vulnerability to this activity and the consequences of such an attack—such as billions of losses in U.S revenue and halts in manufacturing production—are potentially high.[3]

November of 2012 will mark the 10th anniversary of the enactment of the Maritime Transportation Security Act (MTSA) of 2002,[4] which, among other things, called for the establishment of a program to evaluate and certify secure systems of international intermodal transportation, including standards and procedures for screening and evaluating cargo prior to loading and for securing and monitoring cargo while in transit.[5] In 2006, the Security and Accountability For Every (SAFE) Port Act,[6] which amended MTSA, required DHS to develop, implement, and update as appropriate a strategic plan to enhance the security of the international supply chain.[7] To address concerns regarding international supply chain security, U.S. Customs and Border Protection (CBP), a component of DHS, developed a layered security strategy for cargo containers. Core components of the layered security strategy include analyzing information to identify containers that may be at high risk of transporting WMD or other contraband, working with governments of other nations to examine containers CBP has determined to be high-risk before such containers are loaded onto U.S.-bound vessels at foreign ports, and providing benefits to companies that comply with predetermined security measures.

The SAFE Port Act further requires that pilot projects be established at three ports to test the feasibility of scanning 100 percent of U.S.-bound containers at foreign ports.[8] In August 2007, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) was enacted,[9] which requires, among other things, that by July 2012, 100 percent of all U.S.-bound cargo containers be scanned at foreign ports with both radiation-detection and nonintrusive inspection equipment before being placed on U.S.-bound vessels,[10] with possible extensions for ports at which certain conditions exist.[11] Further, in July 2007, DHS issued the strategic

---

[1] 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, DC: January 2011).

[2] Cargo containers serve, in essence, as packing crates and portable warehouses for virtually every type of general cargo moving in the supply chain.

[3] In 2002, the consulting firm Booz Allen Hamilton sponsored a simulated scenario in which the detonation of weapons smuggled in cargo containers shut down all U.S. seaports for 12 days—resulting in a loss of $58 billion in revenue to the U.S. economy along with significant disruptions to the movement of goods.

[4] Pub. L. No. 107–295, 116 Stat. 2064.

[5] See 46 U.S.C. § 70116.

[6] Pub. L. No. 109–347, 120 Stat. 1884.

[7] The SAFE Port Act required DHS to report to Congress on this strategic plan by July 2007, with an update of the strategic plan to be submitted to Congress 3 years later. See 6 U.S.C. § 941(a), (g).

[8] 6 U.S.C. § 981. A similar 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).

[9] Pub. L. No. 110–53, § 1701(a), 121 Stat. 266, 489–90 (amending 6 U.S.C. § 982(b)).

[10] Radiation-detection equipment identifies radiation being emitted from a container, and through nonintrusive inspection CBP can identify anomalies in a container's image which could, among other things, indicate the presence of shielding material.

[11] The 9/11 Act scanning provision includes possible extensions for 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: (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,

plan called for in the SAFE Port Act, entitled the *Strategy to Enhance International Supply Chain Security,*[12] and on January 23, 2012, the administration issued the *National Strategy for Global Supply Chain Security,*[13] which describes a strategy for promoting the efficient and secure movement of goods and fostering a resilient supply chain.

DHS and CBP have taken various actions to enhance maritime container security. As requested, this statement addresses our work in this area and includes the following topics:

- efforts to gather advance information about container shipments to assess the risks of these containers;
- technologies used to protect the integrity of containers and to scan them to detect WMD and other contraband;
- partnerships with foreign governments and the private sector to improve container security efforts; and,
- the status of efforts to scan 100 percent of U.S.-bound cargo containers.

This statement is based on related GAO reports and testimonies issued from April 2005 through July 2011, which addressed various programs that constitute CBP's layered security strategy, along with selected updates conducted from January 2012 to February 2012.[14] For our prior reports and testimonies, among other things, we analyzed CBP documents; reviewed legal documentation; and interviewed foreign government, DHS, CBP, and trade industry officials. We also conducted site visits to select ports that participate in CBP's container security programs and CBP's National Targeting Center—Cargo.[15] Additional details on the scope and methodology for those reviews are available in our published products. For the updates, we collected information from CBP on actions it has taken to address recommendations made in prior GAO reports on which this statement is based. We also reviewed publicly available documents, such as CBP's budget justifications for fiscal years 2011 and 2012 and the administration's *National Strategy for Global Supply Chain Security,* for information regarding DHS's and CBP's plans for implementing the 100 percent scanning requirement. We conducted this work in accordance with generally accepted Government auditing standards.

CBP HAS VARIOUS TOOLS FOR TARGETING U.S.-BOUND CARGO CONTAINERS FOR INSPECTIONS

As part of its efforts to target high-risk cargo containers for inspection, CBP uses various sources of information to screen containers in advance of their arrival in the United States. Specifically, CBP's 24-hour rule requires that vessel carriers submit cargo manifest information to CBP 24 hours before U.S.-bound cargo is loaded onto a vessel. To further enhance CBP's ability to target high-risk shipments, in 2006 the SAFE Port Act required CBP to collect additional data related to the movement of cargo to identify high-risk cargo for inspection,[16] and in 2009 CBP implemented the Importer Security Filing and Additional Carrier Requirements, collectively known as the 10+2 rule.[17] The cargo information required by the 10+2 rule comprises 10 data elements from importers, such as country of origin, and 2 data elements from vessel carriers, such as the position of each container transported on a vessel, all of which are to be provided to CBP in advance of arrival at a U.S. port. Some of the data are required to be submitted prior to loading the container onto a U.S.-bound vessel.[18] Additionally, the United States has worked to expand the program beyond domestic implementation by coordinating with the World Customs Organization (WCO)[19] to incorporate some of the 10+2 data elements into the international supply chain security standards, which are discussed later in this state-

---

or (3) use of the equipment will significantly impact trade capacity and the flow of cargo. See 6 U.S.C. § 982(b)(4).

[12] DHS, *Strategy to Enhance International Supply Chain Security* (Washington, DC: July 2007).

[13] The White House, *National Strategy for Global Supply Chain Security* (Washington, DC: Jan. 23, 2012).

[14] See the list of GAO's related products included at the end of this statement.

[15] The National Targeting Center—Cargo is responsible for targeting high-risk shipments for inspection.

[16] See 6 U.S.C. § 943(b).

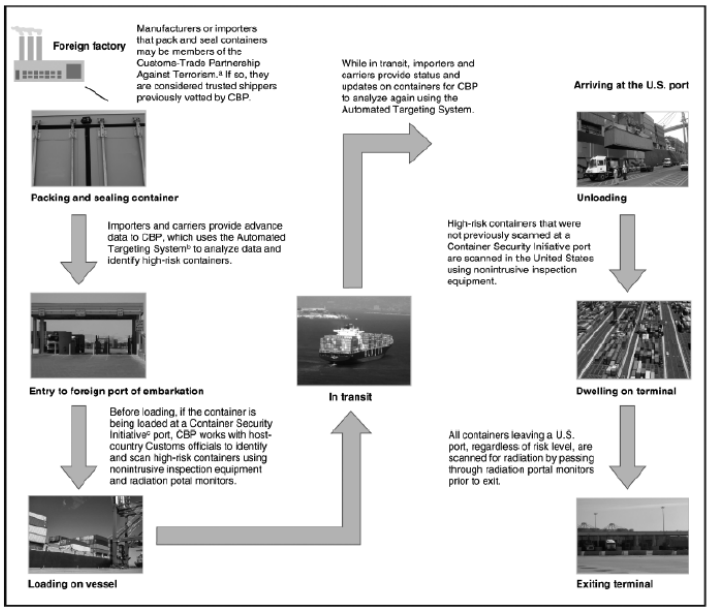
[17] Importer Security Filing and Additional Carrier Requirements, 73 Fed. Reg. 71,730 (Nov. 25, 2008) (codified at 19 C.F.R. pts. 4, 12, 18, 101, 103, 113, 122, 123, 141, 143, 149, 178, & 192).

[18] 19 C.F.R. §§ 4.7c, 149.3(a)–(b).

[19] The WCO is an independent international organization whose mission is to enhance the efficiency and effectiveness of customs administrations.

ment. (Figure 1 illustrates where CBP's container security programs intersect with the key points of transfer in the global supply chain.)

Figure 1: Global-Supply Chain Process



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

[a]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.

[b]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.

[c]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 weapons of mass destruction before they are shipped to the United States. CBP officials identify the containers that may pose a risk for terrorism and request that their foreign counterparts examine the contents of the containers.

Data that CBP collects on U.S.-bound cargo containers and their contents are fed into the Automated Targeting System (ATS)—a computerized model that CBP uses as a decision-support tool in targeting cargo containers for inspection.[20] Specifically, within ATS, CBP uses various data elements to determine an overall risk score for a particular threat in a shipment. CBP officers use these scores to help them make decisions on the extent to which documentary reviews or nonintrusive inspections are to be conducted on cargo containers. In our September 2010 report on the implementation of the 10+2 rule, we recommended that CBP establish milestones and time frames for updating ATS to use the 10+2 data in its identification of shipments that could pose a threat to National security. In response to this recommendation, CBP took steps in January 2011 to improve targeting efforts by updating its targeting criteria in to include risk factors present in the 10+2 data.[21] We recently began a review of the effectiveness of ATS as part of CBP's targeting efforts and plan to issue a report later this year. [22]

[20] For more information on ATS, see GAO, *Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System,* GAO–06–591T (Washington, DC: Mar. 30, 2006).

[21] 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, DC: Sept. 10, 2010).

[22] We are conducting this work for the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives.

DHS HAS MADE SOME PROGRESS IN IMPLEMENTING TECHNOLOGIES TO IMPROVE CONTAINER SECURITY

Container Security Technologies Are Intended to Detect Intrusion and Track Movement

As we reported in September 2010, DHS's Science and Technology Directorate (S&T) initiated four container security technology projects,[23] in part, in response to general MTSA requirements,[24] as well as CBP's need for technologies to detect intrusion and track the movement of containers through the supply chain.[25] Specifically, a CBP study recognized that existing container seals provided inadequate security against physical intrusion (e.g., removing a container door to bypass a container seal) and therefore CBP should develop a technology to monitor and record intrusions on any of the six sides of a container. In September 2010, we reported that DHS had conducted research and development for these projects, but had not yet developed performance standards for them. Specifically, each project had undergone laboratory testing, but S&T had not yet conducted testing in an operational environment to ensure that the prototypes for those projects that had passed laboratory testing would function as intended. Furthermore, S&T's plans for conducting operational testing, did not reflect all of the operational scenarios being considered for implementation. We recognized that successfully testing the performance of these technologies is a precursor to developing performance standards for them; therefore, we recommended that DHS test and evaluate the technologies within all of the operational scenarios DHS identified for potential implementation before S&T provides performance standards to the Office of Policy Development and CBP—DHS concurred with our recommendation and has completed operational testing for two of the four container security technology projects in the maritime environment.[26] S&T officials considered the laboratory and operational testing of both technology projects a success because they were proven to function under one operational scenario, which resulted in the development of performance standards that are necessary to pursue implementation of these technologies. To fully address our recommendation, however, DHS would need to test and evaluate the technologies within each of the remaining operational scenarios it identified for potential implementation. DHS has informed us that it plans to conduct further operational testing and anticipates completing this testing in May 2013.

We also reported on the challenges DHS and CBP could face regarding the implementation of the four container security technology projects.[27] For example, DHS and CBP could face challenges in obtaining support from the trade industry and international partners as it pursues implementation of the security technologies. Specifically, some members of the trade industry we spoke with were resistant to purchasing and using the technologies given the number of container security programs with which they already have to comply. DHS will also need to obtain support from international organizations and the WCO to implement new container security technologies. For instance, for container security technologies to be admitted to foreign countries without being subject to import duties and taxes, as well as import prohibitions and restrictions, the technologies first have to be recognized as accessories and equipment of the containers under the Customs Convention on Containers.[28] The successful implementation of security technologies also depends on the security procedures throughout the supply chain as well as people engaged in those procedures, which are typically documented in the concept of operations. As a result, DHS and CBP could face challenges developing a feasible concept of operations that addresses the necessary technology infrastructure needs and protocols. Container security technologies require a supporting technology infrastructure, including readers to communicate to customs officials whether a technology has iden-

---

[23] Two of the four container security technology projects were to detect intrusion on all six sides of a container; one of them was to detect intrusion on one side (i.e., the door); and, one of them was to track containers and communicate the intrusion to the appropriate officials.

[24] See 46 U.S.C. § 70116 (requiring a program that includes establishing standards and procedures for securing and monitoring cargo in transit, as well as performance standards to enhance the physical security of shipping containers, including standards for seals and locks).

[25] GAO, *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, DC: Sept. 29, 2010).

[26] Laboratory and operational testing has been completed for the project to detect intrusion through the door of the container and the project to track containers and communicate intrusions.

[27] GAO–10–887.

[28] The convention essentially provides for the temporary and admission and reexportation of containers and their accessories and equipment that meet certain requirements without imposition of duties or taxes by any customs authority.

tified an intrusion. Thus, CBP will be faced with determining who will have access to the container security technologies through readers, where to place these readers, and obtaining permission to install fixed readers at domestic and foreign ports. Also, protocols will need to be developed to identify which supply chain participants will be involved in arming and disarming the technologies, reading the status messages generated by the technologies, responding to alarms, and accessing data.

Radiation Detection and Nonintrusive Imaging Technology Can Help Identify Container Contents

To prevent the smuggling of nuclear and radiological materials, as of September 2010, CBP in coordination with DHS's Domestic Nuclear Detection Office (DNDO), has deployed over 1,400 radiation portal monitors (RPM) at U.S. ports of entry. Most of the RPMs are installed in primary inspection lanes through which nearly all traffic and shipping containers must pass before they can exit U.S. ports. These monitors alarm when they detect radiation. CBP then conducts further inspections of the suspect contents at its secondary inspection locations to identify the cause of the alarm and determine what further security measures, if any, need to be taken.

While these RPMs are sensitive and have been effective at detecting radiation, they also have limitations. In particular, in May 2009 we reported that RPMs are capable of detecting certain nuclear materials only when these materials are unshielded or lightly shielded.[29] In contrast, advanced nonintrusive inspection equipment can be used to detect dense material that may be consistent with the presence of certain nuclear materials. CBP already uses nonintrusive inspection equipment to more closely investigate the contents of cargo containers that it has selected for secondary inspection at a U.S. port of entry; however, according to CBP officials, only a small percentage of vehicles or cargo containers are subjected to secondary inspections.

Since 2006, we have been reporting on long-standing problems with DNDO's efforts to deploy advanced spectroscopic portal (ASP) radiation detection monitors, a more-advanced and significantly more-expensive type of RPM designed to replace the RPMs CBP currently uses. GAO last reported on ASP testing in 2009 and found that DHS's cost analysis of the ASP program did not provide a sound analytical basis for DHS's decision to deploy the portals.[30] We also reported that an updated cost-benefit analysis might show that DNDO's plan to replace existing equipment with ASPs was not justified, particularly given the marginal improvement in detection of certain nuclear materials required of the ASP and the potential to improve the current-generation RPM's sensitivity to nuclear materials, most likely at a lower cost.[31] DNDO officials stated that they planned to update the cost-benefit analysis; however, after spending more than $200 million on the program, in February 2010, DHS announced that it was scaling back its plans for development and use of the ASP, and subsequently announced in July 2011 that it was ending the ASP program, which means DHS continues to face limitations in radiation detection. Since DNDO continued ASP testing through 2011, GAO has on-going work to review, among other things, the results of testing of ASP since 2009, lessons learned from the ASP program, and whether DNDO plans to conduct additional ASP testing in the future.[32]

Since 2005, DNDO was also engaged in trying to develop a more advanced nonintrusive inspection equipment system in order to detect nuclear materials that might be heavily shielded. In September 2010, we reported that DNDO was simultaneously engaged in the research and development phase while planning for the acquisition phase of its cargo advanced automated radiography system (CAARS) to detect certain nuclear materials in vehicles and cargo containers at ports.[33] DNDO pursued the acquisition and deployment of CAARS machines without fully understanding that they would not fit within existing primary inspection lanes at CBP ports of entry. We reported that this occurred because, during the first year or more

---

[29] GAO, *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, DC: May 21, 2009).

[30] GAO, *Combating Nuclear Smuggling: Lessons Learned from DHS Testing of Advanced Radiation Detection Portal Monitors,* GAO–09–804T (Washington, DC: June 25, 2009).

[31] GAO, *Homeland Security: DHS Could Strengthen Acquisition and Development of New Technologies,* GAO–11–829T (Washington, DC: July 15, 2011).

[32] We are conducting this work for the Ranking Members of the Subcommittee on Investigations and Oversight and Subcommittee on Energy and Environment; Committee on Science, Space, and Technology; House of Representatives.

[33] GAO, *Combating Nuclear Smuggling: Inadequate Communication and Oversight Hampered DHS Efforts to Develop an Advanced Radiography System to Detect Nuclear Materials,* GAO–10–1041T (Washington, DC: Sept. 15, 2010).

of the program, DNDO and CBP had few discussions about operating requirements. DHS spent $113 million on the program since 2005 and canceled the development phase of the program in 2007.

CBP WORKS WITH FOREIGN GOVERNMENTS, THE PRIVATE SECTOR, AND INTERNATIONAL ORGANIZATIONS TO IMPLEMENT SUPPLY CHAIN SECURITY EFFORTS

As part of its risk-management approach, CBP operates two voluntary security programs—the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C–TPAT).[34] CSI, through partnerships with CBP's foreign counterparts, is designed to target and examine high-risk container cargo as early as possible in the global supply chain. CSI places CBP officers at select foreign seaports to work with host-country customs officials to identify and scan high-risk cargo before it is shipped to the United States. CBP launched CSI in January 2002, and in fiscal year 2007 CBP reached its goal of operating CSI in 58 foreign seaports, and as of October 2011, these ports collectively accounted for over 80 percent of the cargo containers shipped to the United States. In 2005 and 2008, we made recommendations to CBP to further strengthen the CSI program by, among other things, revising its staffing model, developing performance measures, and improving processes for gathering information. CBP generally agreed and took action to implement these recommendations.[35] For example, in response to one of our recommendations, in January 2009, CBP began transferring CSI staff from overseas ports to perform targeting remotely from the National Targeting Center—Cargo in the United States. As part of this effort, foreign staffing levels for CSI decreased from 170 in January 2009 to 86 in April 2011 while 32 positions were added to the National Targeting Center—Cargo. As a result of the changes in its overseas staffing model, CBP has experienced a decrease in operating costs of over $35 million from fiscal year 2009 through fiscal year 2011.

While the CSI program involves partnerships between CBP and foreign governments, the C–TPAT program is a Government-to-business partnership program that provides benefits to supply chain companies that comply with predetermined security measures. Under C–TPAT, CBP officials work with private companies to review their supply chain security plans and improve members' security measures. In return, C–TPAT members may receive benefits, such as reduced scrutiny or expedited processing of their shipments. CBP initiated C–TPAT in November 2001, and as of November 2010, CBP had awarded initial C–TPAT certification—or acceptance of the company's agreement to voluntarily participate in the program[36]—to over 10,000 companies.[37] C–TPAT certified members are then subject to validation whereby CBP verifies that the members' security measures meet or exceed CBP's minimum security requirements. We previously reported that C–TPAT provides CBP with a level of information sharing that would otherwise not be available from non-member companies.[38] In 2008, we made recommendations to CBP to strengthen C–TPAT program management, in part, by developing performance measures and improving the process for validating security practices of C–TPAT members. CBP has since implemented these recommendations.[39]

CBP also partners with international trade and security groups to develop supply chain security standards that can be implemented by the international community. In 2005, the WCO developed the Framework of Standards to Secure and Facilitate Global Trade—commonly referred to as the SAFE Framework—for which the core concepts are based on components of CBP's CSI and C–TPAT programs. As of the publication of the most recent edition of the SAFE Framework in June 2011, 164

---

[34] For more information on CSI and C–TPAT, see GAO, *Supply Chain Security: CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain,* GAO–08–538 (Washington, DC: Aug. 15, 2008).

[35] 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, DC: Jan. 25, 2008) and GAO, *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts.* GAO–05–557 (Washington, DC: Apr. 26, 2005).

[36] Acceptance occurs after a review of the company's security profile and compliance with customs laws and regulations.

[37] Aside from maritime container shippers, C–TPAT members include many top air carriers and freight forwarders.

[38] GAO, *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, DC: Oct. 30, 2009).

[39] 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, DC: Apr. 25, 2008).

of the 177 WCO member countries have pledged to adopt the framework. As part of the SAFE framework, customs administrations may develop Authorized Economic Operator programs that offer incentives to supply chain companies that comply with predetermined minimum security standards. For example, C–TPAT is the designated Authorized Economic Operator program for the United States. According to data from the WCO, as of May 2011, 59 countries, including the 27 member states of the European Union, have implemented or have begun developing Authorized Economic Operator programs.[40]

CBP and the WCO anticipate that widespread adoption of these standards could eventually lead to a system of mutual recognition whereby the security-related practices and programs taken by the customs administration of one country are recognized and accepted by the administration of another. According to CBP, a system of mutual recognition could lead to greater efficiency in providing security by, for example, reducing redundant examinations of container cargo and avoiding the unnecessary burden of addressing different sets of requirements as a shipment moves through the supply chain in different countries. As of June 2011, CBP has signed five Mutual Recognition Arrangements and is currently working toward two more with other customs administrations, according to CBP.[41]

AS THE DEADLINE FOR 100 PERCENT SCANNING APPROACHES, UNCERTAINTY PERSISTS OVER THE FUTURE OF 100 PERCENT SCANNING

The Scope of the Secure Freight Initiative Has Decreased after Facing Numerous Challenges

In response to the SAFE Port Act requirement to implement a pilot program to determine the feasibility of scanning 100 percent of U.S.-bound containers with both radiation detection and nonintrusive equipment, CBP, the Department of State, and the Department of Energy jointly announced the formation of the Secure Freight Initiative (SFI) pilot program in December 2006. CBP selected three ports to implement the SFI pilot program: Qasim, Pakistan; Puerto Cortes, Honduras; and Southampton, United Kingdom.

In October 2009, we reported that while CBP and the Department of Energy had made progress in integrating new technologies as part of the SFI program, progress in implementing and expanding the scanning of U.S.-bound cargo containers at participating ports was limited. Specifically, according to CBP officials, while initiating the SFI program at these ports satisfied the SAFE Port Act requirement to implement the program at three ports,[42] CBP also selected the ports of Hong Kong; Busan, South Korea; and Salalah, Oman to more fully demonstrate the capability of the integrated scanning system at larger, more complex ports with higher percentages of transshipment container cargo—cargo containers from one port that are taken off a vessel at another port to be placed on another vessel bound for the United States. However, these ports faced numerous challenges in implementing the 100 percent scanning requirement, as we reported in October 2009, and some ports that initially agreed to participate in the SFI program did so for a limited time, or on a limited basis.[43] For example, the SFI program began operating in one of the nine terminals at the port of Hong Kong in January 2008 and ended in April 2009. The SFI program was not renewed at the port of Hong Kong based on a mutual decision by the Hong Kong government and DHS, in part, because of concerns that equipment and infrastructure costs, as well as costs to port efficiency, would make full implementation of the SFI program at all of its terminals unfeasible. CBP has since reduced the scope of the SFI program, and currently the only port that continues to operate under SFI protocols is Qasim, Pakistan.

Logistical, technological, and other problems at participating ports have prevented any of the participating ports from achieving 100 percent scanning, as ultimately required by the 9/11 Act, leaving the feasibility and efficacy of 100 percent scanning largely unproven. For example, we reported in October 2009 that while CBP had

---

[40] For more information on the WCO Authorized Economic Operator Program, see *World Customs Organization, Compendium of Authorized Economic Operator Programme,* 2011 edition.

[41] CBP has signed the five Mutual Recognition Agreements with customs administrations of New Zealand, Canada, Jordan, Japan, and South Korea and is working toward more with those of Singapore and EU. For more information, see Department of Homeland Security, Customs and Border Protection, "Mutual Recognition Information," Customs-Trade Partnership Against Terrorism website, (June 2011), accessed January 24, 2012, *www.cbp.gov/xp/cgov/trade/cargo__security/ctpat/mr/*.

[42] The act required CBP to identify three distinct ports through which containers pass or are transshipped to the United States with unique features and differing levels of trade volume. 6 U.S.C. § 981(a).

[43] GAO–10–12.

been able to scan a majority of U.S.-bound cargo containers from three comparatively low-volume ports (Qasim, Puerto Cortes, and Southampton), at the higher volume ports of Hong Kong and Busan, CBP had been able to scan no more than 5 percent of U.S.-bound cargo containers, on average. Additionally, scanning operations at the initial SFI ports encountered a number of challenges—including safety concerns, logistical problems with containers transferred from rail or other vessels, scanning equipment breakdowns, and poor-quality scan images. Furthermore, since the 9/11 Act did not specify who is to conduct the container scans or who is to pay for scanning equipment or operations and maintenance, questions persist regarding who will bear the costs of scanning.

In addition to the challenges CBP faced in implementing 100 percent scanning at the select SFI pilot ports, CBP also faces a number of potential challenges in integrating the 100 percent scanning requirement with the existing container security programs that make up CBP's layered security strategy. The 100 percent scanning requirement is a departure from existing container security programs in that it requires that all containers be scanned before CBP determines their potential risk level.[44] Senior CBP officials and international trading partners say this change differs from the risk-based approach based on international supply chain security standards and accepted practices. Specifically, as we reported in October 2009 and October 2010, foreign government officials have expressed the view that 100 percent scanning is not consistent with risk-management principles as contained in the SAFE Framework.[45] For example, European and Asian customs officials we spoke with told us that the 100 percent scanning requirement is in contrast to the risk-based strategy, which serves as the basis for other U.S. programs, such as CSI and C–TPAT. Further, the WCO, which represents 177 customs agencies around the world, stated that the implementation of 100 percent scanning would be "tantamount to abandonment of risk management." Some foreign governments have stated they may adopt a reciprocal requirement that all U.S.-origin containers be scanned, which would present additional challenges at domestic U.S. ports.

We recommended that CBP perform analyses to determine whether 100 percent scanning is feasible, and if so, the best way to achieve it; or, alternatively, if it is not feasible, present acceptable alternatives. To date, however, CBP has not conducted such a feasibility assessment. CBP has not pursued a feasibility assessment, in part, due to the interagency effort to develop the recently issued National Strategy for Global Supply Chain Security. CBP officials told us in August 2011 that the agency's position was that a risk-based approach to global supply chain security was a more feasible and responsible approach than 100 percent scanning.[46] Further, CBP has not provided any details about any alternatives to 100 percent scanning that DHS or CBP may be considering.

DHS Intends to Issue a Blanket Extension Because 100 Percent Scanning Cannot be Implemented by the July 2012 Deadline

CBP's budget documents and public statements from DHS and CBP officials, along with the elimination of SFI operations at all but one port, indicate that DHS and CBP are no longer pursuing efforts to implement 100 percent scanning at foreign ports by July 2012. While CBP had previously implemented the SFI program and protocols for 100 percent scanning at six ports, it has reverted all but one of these ports to CSI operations, for which CBP focuses its efforts on scanning those cargo containers it identifies as high risk rather than requesting scans of all containers regardless of risk. According to CBP's fiscal year 2011 budget justification, the SFI program is a "helpful but not essential part" of CBP's layered security strategy.

In addition, the budget justification noted that DHS will continue to use and, when appropriate, strengthen other means to achieve the same goals of SFI, such as the 24-hour rule, the 10+2 rule, and C–TPAT. Further, there is no mention of the 100 percent scanning mandate or efforts to meet the mandate in the recently released *National Strategy for Global Supply Chain Security*. Rather, the strategy notes that the Federal Government intends to focus its efforts on "those enhancements that result in the most significant improvement or reduction in risk."

---

[44] For more information regarding the application of risk-management principles as they relate to 100 percent scanning, see GAO, *Maritime Security: Responses to Questions for the Record,* GAO–11–140R (Washington, DC: Oct. 22, 2010), 17–20.

[45] GAO–11–140R.

[46] Additionally, according to CBP, the current SFI budget is focused on maintaining operations at the remaining SFI port in Qasim, Pakistan, and funds are not presently available to conduct a feasibility assessment. The current funding levels may be attributed, in part, to CBP's request to reduce funding for the SFI program. In CBP's fiscal year 2011 budget justification, CBP requested a reduction $16.6 million due to plans to revert three of the SFI ports to CSI operations.

As the July 2012 deadline in the mandate approaches, uncertainty remains regarding DHS's long-term course of action to satisfy the 100 percent scanning mandate. As we previously reported, in the short term, DHS acknowledged it will not be able to meet this deadline for full-scale implementation of the 9/11 Act's scanning requirement and will need to grant extensions to those foreign ports unable to meet the scanning deadline in order to maintain the flow of trade and comply with the 9/11 Act. The 9/11 Act allows DHS to grant an extension to a port or ports by certifying that least two of six conditions exist,[47] and as we previously reported, DHS believes the last two conditions—(1) Use of the equipment to scan all U.S.-bound containers would significantly impact trade capacity and the flow of cargo and (2) scanning equipment does not adequately provide automatic notification of an anomaly in a container—could apply to all foreign ports that ship containers to the United States. Therefore, DHS expects to grant a blanket extension to all foreign ports pursuant to the statue, thus extending the target date for compliance with this requirement by 2 years, to July 2014. To do so, the 9/11 Act requires DHS to report to Congress 60 days before any extension takes effect on the container traffic affected by the extension, the evidence supporting the extension, and the measures DHS is taking to ensure that scanning can be implemented as early as possible at the ports covered by the extension.[48] As a result, DHS will need to notify Congress by May 2, 2012, of any extensions it plans to grant.[49]

Given that the feasibility of 100 percent scanning remains unproven and DHS and CBP have not yet identified alternatives that could achieve the same goals as 100 percent scanning, uncertainty persists regarding the scope of DHS's and CBP's container security programs and how these programs will collectively affect the movement of goods between global trading partners.

Chairwoman Miller, Ranking Member Cuellar, and Members of the subcommittee, this completes my prepared statement. I would be happy to respond to any questions you or other Members of the subcommittee may have at this time.

Mrs. MILLER. Thank you very much, Mr. Caldwell.

That was an interesting testimony, and leads to the obvious question, I guess, and the reason for this entire hearing, as we listened to the first three witnesses talk about all of the various things that have been on-going in the efforts to make sure that we secure the global supply chain, and giving us statistics, et cetera, which are very impressive, based on the workload and the resources available, to be able to accommodate the 100 percent mandate that this Congress has passed.

I guess I would just start by, you were mentioning, Mr. Caldwell, by saying that you had made the recommendation for them to do cost/benefit, risk analysis, et cetera, et cetera, that perhaps if they would have taken some of those recommendations and actually done some of those kinds of things, we would be a little bit further ahead.

But overtaken by events. Believe me, we all understand that. We totally understand that. The purpose of this hearing is just to have a better idea of what kind of events have overtaken us, but whether or not we have any realistic expectation of ever getting to the 100 percent, or if it is even that it is not achievable, as the Sec-

[47] The 9/11 Act scanning requirement authorizes DHS to grant extensions for a port or ports if at least two of the following six conditions exist: (1) Equipment to scan all U.S.-bound containers is not available for purchase and installation; (2) equipment to scan all U.S.-bound containers does not have a sufficiently low false alarm rate; (3) equipment to scan all U.S.-bound containers cannot be purchased, deployed, or operated at a port or ports (including where this is due to the physical characteristics of the port); (4) equipment to scan all U.S.-bound containers cannot be integrated with existing systems; (5) use of the equipment to scan all U.S.-bound containers would significantly impact trade capacity and the flow of cargo; or (6) the scanning equipment does not adequately provide automatic notification of an anomaly in a container. 6 U.S.C. § 982(b)(4).

[48] 6 U.S.C. § 982(b)(6).

[49] Additionally, 1 year after an extension takes effect, DHS would be required to submit a report on Congress on whether it expects to seek to renew the extension. 6 U.S.C. § 982(b)(7).

retary has made testimony to this committee on a number of occasions, where do we actually go from here?

I guess I am, first of all, just trying to understand from a cost—we all recognize it may be optimal but perhaps not realistic from a cost perspective. We have 55 ports in our country, of which there are I think about 700 ports where there is country of origin goods coming into our country.

Do we have any idea at all of what kind of costs we may be looking at, any kind of ballpark figure, in order to—I am not sure who I am actually directing this question to.

Gentlemen, do we have any idea at all of what kind of costs that we are actually looking at, understanding the budgetary constraints that our Nation is facing, but the goal of securing our Nation being our priority as well?

Who might start with answering that question?

Mr. HEYMAN. Let me start by just talking about what the costs that we have to include in that, and then go to some of the specific operational. There are a number of things that we have looked at in terms of the entirety, from end to end, questions about security and resilience.

The implementation of going back to the supply chain, to the manufacturers, and things like C–TPAT, require auditing of facilities and partners to ensure that they are adhering to the security requirements of C–TPAT.

The ports of embarkation require Coast Guard to go and ensure that the international codes have been adhered to, that safety and security for procedures are in place, that counterterrorism programs are in place.

The actual scanning of material, cargo in containers that CBP has, and other programs within the Federal Government, requires that partnerships in foreign countries, with foreign governments. It requires the advanced targeting capability.

Then also, we have the capability at home for screening. So there is technology costs and operational costs. All of those things are so broad and so large that estimate have been not as accurate as people would like.

Mrs. MILLER. I am not looking for an accurate estimate, just a ball park.

Mr. HEYMAN. So this is in the billions and billions of dollars. But let me turn to my CBP colleague, who has the operational arm of that, to actually go into some of the operational costs.

Mr. MCALEENAN. From an operational perspective, we do have some significant experience in terms of the cost of these programs, from these six SFI pilots that we have ran.

Over the course of the 2.5 to 3 years that those pilots were active—and of course, we still have one additional active location in Port Qasim in Pakistan. The DHS alone spent about $68 million on the scanning equipment, on the deployment of it, on software upgrades and all the relevant costs associated with that.

At the same time, our partners at DOE, who are responsible for the radiation and nuclear detection capability aspect of the SFI program, they spent over $50 million. So the total Government expenditures was almost $120 million on those six ports for the short time it was in operation.

Based on our estimates from that experience, we estimate about $8 million per lane, to establish the SFI-type, 100 percent scanning, screening suite of technologies. Now that technology might be improving over time. We are still studying that.

But if you multiply that by the 2,100 lanes at the 700 ports globally that ship direct to the United States, that is quite cost-prohibitive, you know, up to the $20 billion range.

The other aspect of that——

Mrs. MILLER. $20 billion?

Mr. MCALEENAN. Correct, $16.8. The other aspect of that that the assistant secretary mentioned is the cost to the trade. Those estimates have been very high, both in studies from our private sector partners, as well as the European Union and others.

Mrs. MILLER. Okay. I guess I would also ask you, Mr. McAleenan, I was taking some notes here when you were talking about your risk assessments, or the modeling that you are doing. Algorithms, I guess, is the types of things that you are all looking at there.

But one of the things that you were mentioning, if you could just flesh out for me a little bit, is how you gather the information. Then you are looking at targeting technologies from the port of origin, et cetera.

Could you talk a little bit more about what kinds of things, targeting technologies you utilize to make the risk assessments?

Mr. MCALEENAN. Yes, I would be happy to cover that. That is an area of excellence we think that CBP has, in coordination with our intelligence community and other DHS and law enforcement partners.

We take information on cargo shipments as early as possible in the process, both through the 24-hour rule, established after the Trade Act of 2002, as well as the ISF, the Importer Security Filing, the 10+2.

We take that information on shipments, combine it with what we know about the supply chain, the shippers involved in the supply chain, from our trade partnership programs, the C–TPAT, as well as historical data on shipments on certain routes, from certain countries. We manipulate that data using our automated targeting system in a series of sophisticated ways.

One of the most common that we have talked about is our intelligence-based rules. These are specific rule sets that are designed to address each mode. They have different rule sets, for instance, for maritime versus land, air and rail, to identify potential security risks.

We also are using advanced analytic techniques. This is pattern recognition, what is typically called machine learning in the field, to help us model our risk more effectively, beyond just the intelligence-based process.

Of course, we use what we know about the supply chain with our trusted partners, to help reduce the potential for risk on those shipments, as well as the procedures used at the foreign port. So all of that is factored in in an automated fashion, to give us a sense of the risk of individual shipments.

We do that both at our National Targeting Center for Cargo and with our CSI teams deployed abroad.

Mrs. MILLER. Thank you.

My time has expired. But I appreciate your candid information about your best guesstimate about what kind of costs we are looking at, because really it is our job, as Congress, to ask you how much does it cost for you to implement mandates that we are passing.

We need to have a clear understanding of what it is, and understanding the budgetary constraints that we are all dealing with here. Then it is for us to determine, from a priority standpoint, where we are going with our budget here and from National security perspective as well.

With that, I would recognize our Ranking Member.

Mr. CUELLAR. Thank you, Madam Chairwoman.

Mr. Caldwell, you are with the GAO, correct?

Okay. You have been studying the maritime cargo security issue for some time. You know both the legislative requirement, as well as the challenges of scanning 100 percent of in-bound containers.

In hindsight, what different courses could have DHS or CBP have taken to comply with the law?

Mr. CALDWELL. I think in terms of actually setting up the pilot, there could have been more metrics set up to actually measure how long it was taking, the costs, what impact it was having on trade at those individual ports.

I think related to this, they could have come up perhaps with better and validated data on costs, which is still an issue, as we have just discussed. I think, again, if a feasibility analysis, cost/benefit analysis had been done earlier in the process—and it is unclear whether it is ever going to be done at this point—I think it would have made a position to provide specific legislative changes and engage with Congress perhaps earlier.

You know, it is very awkward obviously to do this right before this deadline is approaching in July 2012.

Mr. CUELLAR. Did GAO communicate those recommendations to the Department of Homeland, to CBP, Coast Guard?

Mr. CALDWELL. Yes, we did, particularly with these points the DHS. But they were mainly geared toward CBP, which had the lead in terms of these container programs. So these were recommend in our October 2009 report. We had started talking to DHS earlier, perhaps spring of 2009, about the need for these.

Mr. CUELLAR. Okay. Both CBP and Homeland, what do you all do with recommendations from GAO? Do you just get the recommendations and put them aside?

I am sure you are going to say that you do something with them. But it seems like, you know, I see GAO or an entity like that, that they come with ideas to improve. Then you look at and say, well, this will work; this won't work. You have that dialogue.

But sometimes I get the feeling, with all due respect, that you all know better than anybody else. If you get something from GAO, it is some theoretical, academic report that comes out. What do you actually do with those?

I mean, Mr. Caldwell just mentioned that there were some recommendations. What did you all do with those specific recommendations in 2009? I agree, there is a deadline that is coming up in July of this year. We are coming up to that.

What did you all actually do with those recommendations? Keep in mind, as we are going through this discussion, you know, I am a former businessman. Certainty is important.

In the international business community, not knowing what CBP is going to do, what is going to happen, it affects the certainty. That affects our economy.

What did you all do specifically with the recommendations?

Mr. HEYMAN. So let me answer the general question first, which is what do we do with GAO reports, in terms of the process of adhering to them or not.

We actually have instituted, about 2.5, 3 years ago, a very synchronized dance, in effect, with GAO, where we are trying to get in early. They are trying to get in early to understand the problems. So we are working very closely together.

There is a whole read-in process, where we are all working with them to get them as much data as possible.

On the back end of it, when you are actually implementing—when the GAO is finishing its recommendations, we have given an opportunity to concur or not concur and how we all do it.

We do that in every report. We don't concur with all of the things that they recommend, but we usually provide what kind of corrective action or steps that we all be taking. GAO then follows up, often, with whether we have done that or not.

So there is a process there that we do.

In terms of the cost estimates, the specific question about the cost estimates and how we can do better, by the time I think that report came out, most of the pilot projects had been concluded. Either governments had said they weren't going to continue to implement or they actually had concluded for other reasons.

So actually getting those cost estimates we have—that is the best that we have right now, is from that original data.

Mr. CUELLAR. Okay.

Mr. Caldwell, just roughly, out of the recommendations that you all made, on a 1 to 100 scale, what percent do you think they implemented?

I understand there is a give-and-take. They are not going to accept everything 100 percent. But, I mean, the way I see GAO or inspector general, somebody that comes up with ideas—I see it as a way to improve. You know, how do we make it better, not accepting everything 100 percent.

What would you say on a 1 to 100 scale, roughly?

Mr. CALDWELL. Well, I would say that, you know, our goal within GAO, for example, engaging with the Executive Branch—and this is true with DHS as well—is to get 80 percent of our recommendations implemented.

Mr. CUELLAR. In this specific case, what did they get, roughly?

Mr. CALDWELL. This year, we are not doing very well. Of the I think five recommendations we have, we maybe have two of them partial and the other three—I think also, I mean, one of the recommendations we made that they do a feasibility study, I mean, was a statutory requirement in the SAFE Port Act. It was not just GAO recommendations.

Mr. CUELLAR. So you are saying that on that recommendation, it was a recommendation from your own. There was a statutory requirement, and they have not done it yet?

Mr. CALDWELL. That is correct.

Mr. CUELLAR. Okay. Let me——

Mr. CALDWELL. There are pieces of it, but they need to pull it together. I think the important thing is some of that analysis that feeds that will be important even if we do the blanket waivers, because under the waiver procedure, there is still a reporting requirement that DHS talk about how they plan to achieve—you know, what they are doing to still trying to achieve the 100 percent scanning, and if not, why not?

So that is still some of the justification they are going to need in that analysis, sir.

Mr. CUELLAR. Right. I think, Madam Chairwoman, Members, this is a difficulty, when there is a recommendation; there is a statutory requirement. How do we get your buy-in into this?

One last question, if you don't mind. In regards to the interim Final Supply Chain Security Strategy, required by the SAFE Port Act, the 2007 strategy was—the interim was 128 pages long.

It included details on topics such as defining the problem, strategic objectives, the role of technology, the agency, stakeholders roles and responsibilities, implementation of schedule, priorities and milestones, recovery and resumption of trade, training and exercise requirement.

But the report we just got last month had only 6 pages, which means that there was very little discussion of those topics. I don't understand. Usually when you do an interim report, you build on it.

In this one, you build and you took away. I just don't understand how that comparison was made.

Again, my time is up. But I will take whoever wants to take this one. Mr. Heyman, how do you explain this discrepancy? Or not discrepancy, but how do you go from detail to now a 6-page and I think the first page was more of an executive summary?

It was a managing report of a summary of a summary. So how do you explain that? How do you build down instead of building up?

Mr. HEYMAN. Sir, it is a good question. I would just note——

Mr. CUELLAR. By the way, you saw the other 6 pages. This is the interim report. Then the interim report, 127, 128 pages. You build up on the other one.

Again, I am not saying—maybe this is a perfect example of streamlining and efficiency and effectiveness. But how do you go from an interim that goes into the details that we want to see as oversight, and then come up with this report here?

Mr. HEYMAN. So there is a couple—if I may take a little bit of time on that answer, there is a couple things that we have done differently here than the interim report that should be noted.

First of all, the scale of the report goes beyond just the maritime. It goes into all modes of transportation. It includes resilience as a critical element. It also looks to international engagement on a way that is, frankly, unprecedented.

What we have done in the strategy document is to talk about building on these previous documents. So rather than regurgitate all of them, we tried to make it as simple and as straightforward as possible. That doesn't mean that there isn't more back—there is more behind it.

There are implementation things that we are working on. We have a report to the president that we owe in a year, and things like that. I would hope that we wouldn't get lost in the length of it.

In fact, you know, I think Eisenhower's strategy for World War II was two words, which was "Europe first." But we have a lot of things that go beyond that.

We are, in fact, actually implementing now things like the Supply Chain Security Initiative the Secretary put forward, that fits into the global strategy the President put forward.

All those things come together.

Mr. CUELLAR. Yes. I can summarize two words into one: "win". But what I am saying is this is something that should be a guideline to what we are doing. I am just a little disturbed by what I am seeing here, especially recommendations from Mr. Caldwell, and not meeting a lot of them.

But again, Madam Chairwoman, I thank you for indulging me on this very important issue. Thank you.

Mrs. MILLER. Thank the gentleman.

The Chairwoman will now recognize the Ranking Member of the full committee, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Madam Chairwoman.

Mr. McAleenan—McAleenan, okay—the goal of this Congressional law was to give us, within a reasonable period of time, 100 percent scans on container shipments coming to the United States.

Where are we at this point in that 100 percent?

Mr. MCALEENAN. In terms of the total percentage, sir?

Mr. THOMPSON. Yes.

Mr. MCALEENAN. Okay. Our CSI program covers 80 percent of global trade to the United States. In terms of the actual scanning, we do about 45,000 inspections last year through our CSI ports prior to loading on vessels. That is a little bit less than 1 percent of the total cargo headed to the United States.

Then we scan an additional 4 percent upon arrival domestically in the United States.

Mr. THOMPSON. All right. In layman's terms, what percent cargo that is coming to the United States right now is not scanned?

Mr. MCALEENAN. In the maritime environment, sir, in terms of physical scanning, that would be the vast majority, over 95 percent.

Mr. THOMPSON. All right. Why not?

Mr. MCALEENAN. Well, we have been discussing with you, sir, and your committee for several years the complexities of this process and the tests that we have undertaken with SFI to examine the feasibility of the physical scanning, in particular.

At the same time, we have been aggressively pursing the layered approach, focused on the targeting and intel, coordination through CSI with our foreign partners, conduct those exams on high-risk shipments before they are loaded, working with international community on standards——

Mr. THOMPSON. I understand.

Mr. MCALEENAN [continuing]. So forth.

Mr. THOMPSON. Taking whatever you are doing to—whether it is high-risk shipments or anything like that, at this point in this hearing today, is there any shipments using your protocol that is coming to the United States that we don't know what is in it?

It is not a complex—of what you are saying—is the layered approach, where you are scanning, where you are taking high-risk, I want to know what the number is.

Mr. MCALEENAN. We have stated contents on all shipments destined to the United States. Through the ISF 10+2 Filing, we also have the carrier explaining both the location on the vessel of the container, as well as the container status message, where it is in the process.

The combination of those two data elements allows us to identify any un-manifested containers that are on a vessel. We address those with a carrier upon arrival.

Mr. THOMPSON. Wait, wait, wait. Hold, hold it.

So your testimony to this committee is that there is no container shipment coming to the United States that we don't know what is in it?

Mr. MCALEENAN. Sir, I think that is too strong a statement. What I have explained is that we have requirements——

Mr. THOMPSON. I understand requirements. Are you doing 90 percent? Are you doing 85 percent? Are you doing 95 percent?

I want to know where we are toward 100 percent standard. Whatever protocols you are using, that is fine. But I want to know where the gaps are right now.

Mr. MCALEENAN. There are very little gaps on information. We have very high compliance with——

Mr. THOMPSON. Well, what is the little. Give me the little.

Mr. MCALEENAN. The 24-hour-rule compliance is over 99 percent. ISF compliance, as a relatively new program, that is at 92 percent.

That is where we get the information on the cargo shipments in the maritime environment. So it is very, very high compliance on both of those programs.

Mr. THOMPSON. Mr. Heyman, do you agree with that?

Mr. HEYMAN. Yes. Almost 100 percent of all things coming to the United States are known to us, in terms of what is in the manifest, what is the lading. We then use that information to do a risk analysis.

Mr. THOMPSON. So we are 99 percent of the container shipments that come to the United States, its your testimony before this committee, meets the requirement that we set forth in the 2007 law?

Mr. HEYMAN. No, that is not what I was saying. What I was answering—the question was whether we knew of all of the stuff that was coming to the United States. The answer is generally yes.

Mr. THOMPSON. When you said knew about—I am not saying of all the stuff. Do you know what is in the containers?

Mr. HEYMAN. Yes.

Mr. THOMPSON. You do?

Mr. HEYMAN. So the——

Mr. THOMPSON. At 99 percent?

Mr. HEYMAN. Yes. The question that the law puts forward is to whether the information that we receive is accurate, and whether, in fact, somebody has tried to fraudulently put material into a container or misrepresent what is in a container.

That is what we try to identify. In fact, we have done it to great success. About 11,200 narcotics seizures last year.

Mr. THOMPSON. No, no. I am not asking for that kind of data. I am just trying to give the public the confidence that the law Congress passed saying we want 100 percent, that you are telling this committee, from what I understand, that you are 99 percent there.

Mr. HEYMAN. No, in terms of the 100 percent scanning mandate, Congressman, that mandate, as we have testified over a number of times over the last several years, poses significant operational, diplomatic, financial, and technical challenges.

Mr. THOMPSON. Well, that is fine. So where are you to do the 100 percent? What percent along the way are you?

Mr. HEYMAN. What my colleague has just testified to is that we are doing approximately 5 percent of the——

Mr. THOMPSON. You are 5 percent.

Mr. HEYMAN. Approximately, yes.

Mr. THOMPSON. All right. So what are we doing for the other 95 percent?

Mr. HEYMAN. So those are what we have done. They go through the advanced targeting system to be identified as not part of a high-risk containers that require additional inspection.

The inspection process, remember, is first to look at whether the manifest is accurate, second to look at whether there is any threat information, third to look at the opportunity for non-intrusive inspection. Then ultimately we may have to open that up.

That is the most difficult course.

Mr. THOMPSON. But that is the process DHS put together. That was not the process that Congress directed.

Mr. HEYMAN. Actually, that is the process that was put in place for the pilot project that Congress asked us to do.

Mr. THOMPSON. Yes, but the pilot projects are done. So you have now taken that and made that the policy, based on what you just said.

Mr. HEYMAN. I am not sure I understand.

Mr. THOMPSON. Mr. Caldwell, let me ask a question of GAO. Are you comfortable with the responses you have heard, that 99 percent of the cargo or container shipments coming to the United States, we know what is; we know what is in it?

Mr. CALDWELL. No. Let me maybe interpret what I am hearing here.

Mr. THOMPSON. No? Don't interpret it. Just stick with the facts. Why are you not?

Mr. CALDWELL. For the majority of the containers, we have the manifest. It doesn't look suspicious, that is where the scrutiny stops.

Now in many cases, this may be a standard shipment from a manufacturer overseas into a Target store here in the United States, maybe towels, textiles, anything else. But as far as assurance of what we know in there, we have the manifest and the manifest only.

Mr. THOMPSON. So other than the manifest, we don't know.

Mr. CALDWELL. That is correct, unless there is actual scanning.

Mr. THOMPSON. Thank you.

Mrs. MILLER. Thank the gentleman.

At this time, the Chairman will recognize the gentleman from South Carolina, Mr. Duncan.

Mr. DUNCAN. Thank you, Madam Chairwoman.

Let me just pause to say thank you for arranging a tour of the Port of Baltimore with Customs and Border Protection and the Coast Guard recently, where you and I had an opportunity to witness some of the things that the Ranking Member is talking about with scrutiny of manifest, looking at country of origin, stops of the ship that is carrying containers, possible interdiction multiple places along the way, and then the active screening there in the port for radioactive material, chemical and biological issues.

So when you think about the number of ports in this country and the number of containers that come in, I am amazed that we are able to do as well a job as we do. I commend the gentlemen that are doing that, implementing the policies of this country every day to keep us safe.

So thank you. Thanks for educating me.

I guess the question I have—is it McAleenan?

Mr. MCALEENAN. McAleenan, sir.

Mr. DUNCAN. Thank you. I wasn't here for the introductions, Madam Chairwoman, so I apologize.

Can CBP effectively screen high-risk shipments in a way that expedites legitimate commerce? Because from what I saw, there is a stop-and-go process. I know that we have targeted certain containers and certain countries of origin, and we are trying to do a very good job there.

But I am very concerned the speed of commerce and expedition of that. So can you screen high-risk shipments in a way that expedites legitimate commerce, while at the same time ensuring the security of the United States? If you will touch on that?

Mr. MCALEENAN. Yes, I believe we can, Congressman. Our layered approach is designed to do precisely that.

For the vast majority of cargo that we determine to be low-risk, based on our analysis of intelligence, the information provided on those cargo shipments, our knowledge of the supply chain and our knowledge of the parties involved in that transaction, those are released and fed to their destination, the engine of our economy, right away, usually before arrival.

For those very small percentage of cargo that we think might be risky, or that we don't have enough information on them and we want to take a further look at, we do try to address that potential risk at the earliest possible time in the supply chain.

Forty-five thousand times last year, that was done before the cargo was even laden on the vessel in the foreign port. Another 5 percent of cargo is examined at the U.S. port of arrival. We try to even do those examinations in the most efficient way possible.

We use a non-intrusive inspection technology, which is a gamma imaging and X-ray device, as you probably saw at the Port of Baltimore, to do the initial exams on cargo that we determine might be

high-risk. That is a very quick process that we can scan the cargo efficiently.

If we don't see any anomalies, if the picture looks consistent with the commodity that we expect to be in that container, we are able to allow that to proceed into the commerce. It is only a very small percentage, tiny percentage that still remains of concern, that we actually do a full examination in what we call de-vanning, which is emptying the container and looking at all the contents.

So that layered approach is designed to do precisely what you asked about, Congressman, in terms of facilitating that trade while securing it.

Mr. DUNCAN. I appreciate those efforts and you clarifying that.

You know, it seemed like there was going to try to be a gotcha moment a minute ago, asking for 100 percent or 99 percent. There is no way that any country in the nation or in the world can fully screen every container, based on the sheer number that are coming into this country.

So I think scrutinizing the manifest, understanding the country of origin, understanding the history of that particular shipper or that particular manufacturer or that particular importer, is critical.

So watching you all implement those different steps, and saying this container came from X, Y, Z country, but it made stops at country Z and country Y before it came to the United States. Maybe it was offloaded there and held for a while, and then put on another container ship.

Tracking that container the whole way, and understanding that we need to pull that out of the line, we need to scrutinize it a little bit further, even to the point of possibly unpacking it, is an amazing undertaking.

So trying to see a gotcha moment of 100 percent of the containers, and we know everything that is in there—no. That is ridiculous.

We don't know how many towels are in there other than what the manifest says. But you guys do a tremendous job.

Madam Chairwoman, we saw it, that looking for threats, assessing those threats.

So the question I have for Mr. Caldwell is: In your estimate, what do you think it would cost the Government to fully implement 100 percent cargo screening? What is the dollar figure on that, sir?

Mr. CALDWELL. Well, we talked a little earlier about a figure of $20 billion. That is the same figure we had reported in 2009.

Mr. DUNCAN. $20 billion?

Mr. CALDWELL. $20 billion. Now it is a little unclear who would pay this. The SAFE Port Act and the 9/11 Act do not specify who would pay it, which is a large issue, of course, with that amount.

Mr. DUNCAN. Ultimately the consumers are going to pay, because import/exporters are going to pass those costs on. That is obvious to most folks.

I am out of time, Mrs. Chairwoman. I yield back, Madam Chairwoman.

Mrs. MILLER. Thank the gentleman.

At this time, the Chairwoman would recognize the gentle lady from California, Ms. Sanchez.

Ms. SANCHEZ. Thank you, Madam Chairwoman. Again, you are doing a good job.

Mrs. MILLER. Thank you. So are you.

Ms. SANCHEZ. I would first ask the gentle lady, I have had the privilege of being able to go and take a look, having chaired this subcommittee before, to many of the ports abroad, to see what conditions they work under.

I would just say that I think aside from trying to take a look at some of the major ports we have here, this subcommittee might think about taking a look at the major ports that actually export to us, and see what conditions there are.

There is a big difference between Mumbai, for example, the Port of Mumbai, and Singapore. That allows us to understand it is difficult to get to this 100 percent scanning issue.

In fact, we have just learned, and we have known for a while that it is just 5 percent or so that we scan. I understand the layered approach. I was one of the people who pushed the C–TPAT, for example.

But, you know, there is still this uneasiness, at least for me, about relying on the manifest for a majority of what is going on, and just looking for abnormal patterns and risk analysis towards that, and then taking a look at that.

So I think it is very difficult to get to 100 percent screen. But at the same time, there is still a lot out there that we are missing. For example, it is my understanding that of the cargo at Container Security Initiative Ports determined to be high-risk, Customs and Border Protection scans are otherwise resolved 96 percent of the shipment that goes overseas.

That means that 4 percent of those, or in fiscal year 2011 a little under 2,000 shipments, were high-risk cargo that weren't examined before they arrived to the United States. As somebody who lives 20 minutes away from Long Beach/L.A. Port, that is a big concern.

If there is a dirty bomb or something else in there, I don't want it reaching here. I really do want to push it out and have that happen out there.

So that is one of the questions I have, is can you please discuss that particular issue?

Then my second question would be that Secretary Napolitano has testified that the requirements of H.R. 1, recommended by the 9/11 Commission, could not be met for several reasons, including that the technology does not exist for 100 percent effective and efficient cargo screening.

So is that the Department's position today, that we don't have the technology to do an efficient and effective, fast, 100 percent screening?

It is also my understanding that the Domestic Nuclear Detection Office is developing a plan for evaluating and testing muon tomography as part of the Advanced Technology Demonstration Program. This program has been installed in three ports—Bahamas—to demonstrate as a private/public project in the operational environment.

So has the Department taken a look to see if they want to participate in this test to see if, in fact, that technology works, and whether we can get it put in here to the United States?

So these would be my three questions, Madam Chairwoman.

I will leave it to any of you to answer those.

Mr. MCALEENAN. Okay. I will take your first, Congresswoman.

Your numbers are correct on the 96 percent of exams which are accepted by our foreign partners in the CSI ports for examination. The 4 percent—there are challenges sometimes in the timing of the request.

Some of our partners aren't able to respond during the hours that we need them to, before the container is ladened. It does mean it gets ladened without an inspection, even though we have asked for it.

Ms. SANCHEZ. It arrives in my Long Beach Port, let us say.

Mr. MCALEENAN. Correct. That happened about 1,780 times last year, out of the 10.5 million total cargo shipments to the United States. So it is a very tiny percentage that we have targeted with CSI, but the foreign governments aren't able to respond.

Ms. SANCHEZ. But it is still 2,000. If happens to be one of those that gets put on a truck that goes through the 5 Freeway in my neighborhood——

Mr. MCALEENAN. Understood. The definition of high-risk does not necessarily mean that it is a risky shipment. In fact, we have not found an explosive device or terrorist weapon in all of these shipments that are targeted.

These are based on anomalies in the supply chain. They are based on intelligence factors. In most of all of the inspections, the vast majority resolve to no concern.

So, you know, to your point, we would like to get 100 percent response in this from our CSI partners. The 96 level is our highest historically that we have achieved.

We continue to work with our partners to try to get to that 100 percent level on the CSI ports.

Ms. SANCHEZ. Thank you.

Mr. HEYMAN. To get to your other two questions, first, let me just agree with you. I think I would recommend a visit to these ports. If you have seen one port, you have seen one port. I mean, they are so different.

One of the things that has been challenging to us is that diversity. A terminal operation in one port can be different from another terminal operation in the same port or even other ports.

So in terms of the cost of the technology and things like that, it is not just that. It is also how you configure your operations on the terminal; what is the footprint? All of those things need to be factored into it.

They are all problematic.

Ms. SANCHEZ. Yes, because every port was made in a different way. You have a different footprint. You can't put the same standardization in.

Mr. HEYMAN. Correct. You know, they weren't designed for——

Ms. SANCHEZ. This.

Mr. HEYMAN [continuing]. This, exactly. Furthermore, the challenge, of course, that we are on—we are looking to do this in foreign countries, and the diplomatic challenges.

I think in the pilots, if you look at them, we had labor issues in South Korea. We had what I just described the terminal operations

were challenging in other ports. United Kingdom expressed that they were not interested in pursuing this.

So there are foreign diplomatic challenges, not just the technical ones or the cost ones. I don't want to belabor the point.

Let me get to your second question about the technology. We have to look at technology as a possible solution down the road. We always want to look at that as a possible long-term solution. It helps drive down costs. It may increase efficiencies. It may increase also the speed in which goods flow through our ports.

So we are looking at that. We are partnering with other agencies and within our own strategy, looking to do additional investments in technology and technology development. We all see where that goes in the long term.

Ms. SANCHEZ. So is it still the Department's official position that the technology does not exist to do the 100 percent screening?

Mr. HEYMAN. The technology that we have—well, no, there is technology that exists today that has challenges, all of the ones that I just described, and including challenges I didn't describe, such as false positives, which end up——

Ms. SANCHEZ. Right. I understand.

Could you answer for the record, in writing, the third question that I had about the free port situation, what you know about it, whether you are involved in it, whether you think you are going to get involved in it?

Mr. HEYMAN. Happy to do that.

Ms. SANCHEZ. Thank you.

Thank you, Madam Chairwoman.

Mrs. MILLER. Thank the gentle lady.

The Chairwoman now recognizes Mr. Broun from Georgia.

Mr. BROUN. Thank the Chairwoman.

This hearing, as well as many others, have pointed out something I have long said here in this committee. That is that the Department of Homeland Security has it totally wrong.

We are spending billions of dollars. In fact, I submit we are wasting billions of dollars looking for objects, instead of looking for those who want to harm us.

We would be much better off as a Nation, much more secure as a Nation if we would spend the money in human intelligence, focusing on those who want to harm us. We have got to stop patting down grandma and children, and start looking at airports for those who want to do us harm through the aviation sector.

We need to stop looking at all this technology to try to get to 100 percent when we can only get 5 percent, by really focusing on those entities throughout the world that want to harm us. We are not doing that.

We are wasting billions of taxpayers' dollars. We are giving them a false sense of security. We are giving them a message that this country is going to be free from having dirty bombs, as Ms. Sanchez was talking about.

We are wasting the taxpayers' money. It is actually preposterous to continue looking for objects. We need to totally change our focus, whether it is with shipping into our ports, across this country, around the world. We need to start focusing on those who want to harm us.

Having said that, I have got just a couple of questions. Why is there such a lack of specifics in the administration's new "National Strategy for Global Supply Chain Security"? Anybody.

Mr. HEYMAN. The strategy represents the highest level of fidelity for what we need to do to accomplish our interests in ensuring the security and resilience of global supply chains. There is obviously a much richer and deeper programmatic implementation that goes underneath that.

What the strategy tries to convey is the idea of all of the preceding programmatic and strategic efforts that have gone before, that this strategy builds upon. Rather than belabor—and oftentimes you do list some strategies as you talk about all of the authorities and everything that goes before that.

We tried not to do that because we wanted people to read it. That said, we would be happy to give you a more detailed brief at some point of all of the things that we are doing and have been accomplishing in the last year.

Mr. BROUN. Well please do, because business has a very great difficulty dealing with your lack of specifics.

Why has the administration spoken against 100 percent scanning? In some cases, they have even waived the mandate, but has not requested that Congress repeal the mandate.

Mr. HEYMAN. At this point, one of the things that we have done in the last several years, which I think is important for people to recognize, is put in place programs that actually allow us to do much better risk management.

If you look at the ATC, which my colleague described, the Advanced Targeting Center, and the information, the 10+2, which allows us to do much better analysis, we are probably—I don't know, eons—much further down the road in terms of our ability to identify high-risk and interdict high-risk cargo than we were 5 years ago.

So in many regards, we are moving in a direction which allows us to be practical and responsible in the implementation of the law.

Mr. BROUN. In the Science Committee, we have looked at a number of the technologies that have been developed, you utilized, and some that are just sitting in warehouses. I would like to have from the Department a run-down of how much money has been spent on technologies that have been used and discarded as being effective.

How much money has been even spent and not even utilized, is sitting in warehouses? If you please provide those data for me, I would be very interested to see those. Because I know from a Science Committee perspective, there have been a lot of technological proposals that the Department has purchased, and have just never been employed.

But I encourage the Department to change tracks. We have got to focus on terrorists, instead of focusing on objects. TSA just takes great pleasure in talking about how many weapons have been found in airports and talking about the successes that they have had.

But we have let terrorists on airplanes. We are not doing our job to keep America safe. The Department is looking in the wrong direction when we are looking at objects.

We need to look at people, those people who want to destroy us, and those people groups that want to destroy us. I am not talking about looking at every Muslim, every person from Middle Eastern descent.

We need to look at terrorists, instead of looking for the objects that the Department of Homeland Security is doing now. We are wasting billions of taxpayers' dollars in doing so.

So I encourage the Department to change tracks. I have told the Secretary that she is wasting money and that the whole philosophy of the Department is totally wrong.

We need to look at terrorists. We need to look at those people who want to harm us, instead of trying to look at objects and keep them from coming in this country, or getting on airplanes, boats, or ships, or trains.

We aren't even looking at those other things, just at aircraft.

I yield back, Madam Chairwoman.

Mrs. MILLER. Thank the gentleman.

The Chairwoman now recognizes the gentle lady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank the Chairwoman and the Ranking Member.

To the witnesses, let me ask you a first question of everyone. I was trying to catch the gentleman from Georgia's comments about wasting money, but I know that you can't put a price in America on loss of life.

Obviously, the issue of property can sometimes generate enormous catastrophic impact on communities. So let me ask the members of this panel representing a number of entities that are involved in I believe the mandate of 100 percent cargo screening that was supposed to take place in January 2012.

Secretary Heyman, do you have the resources? Please don't tell me that it is not in my area. You are here to talk about cargo screening and et cetera. So it is your impression that the Department has the resources, the money right now to make good on the mandate of 100 percent screening?

Mr. HEYMAN. No, ma'am.

Ms. JACKSON LEE. Thank you.

Okay, we are always getting this. Mr. McAleenan.

Mr. MCALEENAN. McAleenan, right.

Ms. JACKSON LEE. Yes, thank you. Kevin, my good friend. No.

Mr. MCALEENAN. That works, Congresswoman.

Ms. JACKSON LEE. A distinguished name. Your answer to that, please, sir?

Mr. MCALEENAN. My answer would be the same, ma'am.

Ms. JACKSON LEE. Okay.

Admiral Zukunft.

Admiral ZUKUNFT. We are not in the container screening. But an element that wasn't introduced was the foreign port assessments that we are——

Ms. JACKSON LEE. Again, that is correct.

Admiral ZUKUNFT. Yes, well 153 nations, four that we don't do trade with. So that is just another piece of it. Then we are embedded with CBP.

We screened 28.5 million people last year. Getting back to the Congressman from Georgia's question, as looking at those people. So one, are there holes in the fence line, so to say, in a foreign port, where there are not good access control points, where someone can enter that facility and then introduce an object into a container that is not in a manifest?

Then screening people; is there somebody on that vessel that may do the same?—and looking at that history. Then impose conditions of entry on those vessels that may enter a U.S. port.

Then it really comes down to let us stop that threat before it enters a U.S. port. Let us not stop it at the terminal.

Ms. JACKSON LEE. So do you have——

Admiral ZUKUNFT. So we currently have the resources to do these foreign assessments. We have roughly 60 individuals that are dedicated to doing foreign port assessments. Our challenge is the resources that it would take to actually stop the threat before it enters U.S. waters.

So that is where, as you have heard our comment on State, time and again—that is where our rubber meets the road.

Ms. JACKSON LEE. So you have the personnel right now and you have the resources. Is there a time when you expect those resources to run out?

Admiral ZUKUNFT. Not on foreign port assessments. In fact, we have been able to advance those objectives working with foreign partners, particularly in the European Union.

Ms. JACKSON LEE. This is under your Coast Guard funding?

Admiral ZUKUNFT. It is.

Ms. JACKSON LEE. Mr. Caldwell, you are likewise with the Government Accountability. Do you think DHS made a assessment of the resources that they have to meet the mandate that was given to them?

Mr. CALDWELL. Not for the 100 percent, no, ma'am.

Ms. JACKSON LEE. Is anyone in your shop looking at that issue? That is part of what may be the potential problem. Is it not?

Mr. CALDWELL. Well, every year, we do analyze the budgets, provide advice to Congress and committees such as this.

Ms. JACKSON LEE. In the most recent budget that you have analyzed, what is your guess on that? When I say recent, the most recent one that we may have had, because we don't have a budget as we speak.

Mr. CALDWELL. Could I be very specific?

Ms. JACKSON LEE. Yes. You can, sir.

Mr. CALDWELL. The 2012 budget versus the 2011, there was a 50 percent reduction in international cargo screening requested by the administration.

Ms. JACKSON LEE. Thank you very much.

Requested from the administration and then ultimately what occurred? Do you have a next step of what they actually received?

Mr. CALDWELL. Well, part of this was a shifting of funds from actually people in the ports, like in the CSI port, back to the National Targeting Center. From our perspective at GAO, while some people need to stay in those ports to have relationships with the host countries, that in general, the targeting purposes, that can be done

much cheaper and more efficiently back here at the National Targeting Center, ma'am.

Ms. JACKSON LEE. Thank you.

Would the Chairwoman indulge me for just one last question, please? I would appreciate it, Madam Chairwoman.

A study produced by Booz Allen Hamilton last year indicated a 30-day closure of the Port of New York and New Jersey would result in an economic impact on the U.S. GDP of over $5 billion and loss of 50,000 jobs.

Whether in New York, in my hometown of the Port of Houston, Houston port, or in any of the other major ports across the country, a terrorist incident that closes our Nation's ports would have a devastating economic affect in the United States and around the world.

Understanding these potential economic growth impacts—potential economic impacts, can we afford not to increase the security of maritime cargo arriving on our shores?

I want to point that to the assistant secretary and to the assistant commissioner.

Mr. HEYMAN. Thank you for that, Congresswoman. That is right. This is one of the reasons this strategy is being put forward. In fact, the disruptions to ports, the disruption to commerce, the disruption to supply chains is going to happen at some point.

We have seen it recently with the tsunami. We have seen it with the volcano last year. We have seen it with terrorism.

One of the things we have tried to do in this strategy that is different and that is important to recognize is to internationalize the solution. That is to say we have gone to and are going to multilateral organizations, World Customs Organization, ICAO, IMO, Universal Postal Union.

We are working bilaterally and saying, look, we need to raise standards. No one government, no one private sector firm, nobody is going to be able to solve this on its own. It has to be a community effort.

That is why one of the things we are going to be working on and having been working on is to internationalize this.

Ms. JACKSON LEE. Have you given up on 100 percent screening?

Mr. HEYMAN. We are continuing to operate under the law.

Ms. JACKSON LEE. Can Mr. Commissioner just finish the answer? It was two of those that I posed the two. Commissioner, thank you.

Mrs. MILLER. Okay.

Ms. JACKSON LEE. Thank you.

Mr. MCALEENAN. I would just say we must maintain our robust, layered approach to enhance cargo security. We have got to continue to improve.

We take the GAO's comments very seriously and have used them, as Mr. Caldwell testified, to improve our programs over the course of the past 5 or 6 years.

In fact, the CSI recommendation that they made has saved us $35 million a year without diminishing our security with the CSI program. So that is a—maintaining our structure and expanding it, improving it is absolutely essential.

Ms. JACKSON LEE. I thank the Chairwoman and the Ranking Member.

I thank the witnesses. I yield back.

Mrs. MILLER. Thank the gentle lady.

The Chairwoman now recognizes the gentle lady from California, Ms. Richardson.

Ms. RICHARDSON. Thank you.

First of all, I would like to start off my comments by thanking Chairwoman Miller and Ranking Member Cuellar for supporting my participation today in the hearing.

Second of all, for the record, I would like to note that Representative Rohrabacher is the one who represents the Port of Los Angeles and Long Beach, which is known as the San Pedro Complex. It is the largest port in the United States, of which I will be focusing my comments today.

I also want to note for the record that at a full Homeland Security Committee hearing on February 25, 2010, I questioned Secretary Napolitano on the progress of the 100 percent container screening. On June 16, 2011, as Chairwoman of the Subcommittee on Emergency Communications, Preparedness, and Response, myself and committee Members submitted a letter to the Secretary regarding the impending deadline of the screening.

Then again on March 3, 2011, I asked Secretary Napolitano about the 100 percent cargo screening. So this has been a concern of mine for quite some time.

With all due respect to some of our folks here who are testifying, for those of us who live in these communities, the port complex itself is in Mr. Rohrabacher's district. However, all of the land portion and all of the impacts of the port, meaning trucks and activity, for example, in the Port of Long Beach is in my district.

So I take it pretty seriously.

Madam Chairwoman, for the record I would also like to point out that not speculating ideas, but according to the University of Southern California's Homeland Secure Center, a preliminary economic report was performed back in 2003 due to the strikes that we had, the labor strikes in 2003.

It was recorded at that time that $1 billion a day was lost, based upon the closure of our ports. So with all due respect to the people who are testifying, when we say a number of $16, $20 million, whatever it is, when you keep in mind that we lost $11 billion in 2003, and that was a labor issue; that wasn't even if there were infrastructure damages.

So I am not putting aside the cause that we need to consider these costs. Which leads me to my first question. If you could do yes and no as much as possible, I would appreciate it.

Mr. Heyman, to your knowledge, has the Department conducted a feasibility analysis, based upon costs, as Mr. Caldwell has referenced?

Have you guys done that, yes or no?

Mr. HEYMAN. We have not done a full feasibility study.

Ms. RICHARDSON. Okay. Thank you. My next question would be, Mr. Heyman, to your knowledge, have any steps been taken—are any steps being taken at this time to achieve the SAFE Port Act 9/11 Recommendations of 100 percent scanning in the Department?

Mr. HEYMAN. Yes. We have submitted a report. We can make sure you get a copy on that.

Ms. RICHARDSON. Let me make sure you are clear on the question that I am asking. This report will reflect what steps you are taking to achieve the 9/11 recommendations of 100 percent scanning?

Mr. HEYMAN. This report reflects all of the SAFE Port requirements and how we are implementing it.

Ms. RICHARDSON. How you are working to achieve 100 percent scanning?

Mr. HEYMAN. The report talks about what we have done to achieve 100 percent scanning to this point.

Ms. RICHARDSON. Okay.

Commissioner, is it true that the CBP relies upon host governments, with their customs personnel in relevant foreign countries, to resolve issues of containers that are deemed high-risk?

Mr. MCALEENAN. Yes. We work with host nation authorities that are sovereign in those ports, and oftentimes observe the examinations of participants.

Ms. RICHARDSON. Is it true that the CBP does not require scanning at these ports?

Is it true that you do not require scanning of the high-risk containers out of these various ports, these foreign ports?

Mr. MCALEENAN. Our CSI folks are operating with requests, as opposed to requiring authority to examine.

Ms. RICHARDSON. So it is correct of my question that you do not require scanning at these ports. Is that correct?

Mr. MCALEENAN. We do not have the authority to force a sovereign nation to take action on our behalf.

Ms. RICHARDSON. Okay. Again building upon Ms. Sanchez, it is true that 4 percent of the cargo identified at these ports have been identified as high-risk and have arrived in the United States without being scanned. That is correct?

Mr. MCALEENAN. That is correct, 1,750 shipments last year.

Ms. RICHARDSON. Okay. Mr. Heyman, you testified about all these wonderful international relationships. However, when I asked the Secretary and when I also asked Ambassador Kirk, in these trade agreements that we recently approved, was there any effort to work with these foreign countries to establish a scanning process?

The answer in both of those was no, didn't know, would get back to us. Do you know anything different than that?

Mr. HEYMAN. I do not, but I can get back to you, if you like.

Ms. RICHARDSON. Okay.

Finally, Madam Chairwoman, I would just like to build upon Mr. Broun's request of not only requesting the information of costs of some of the technology of what is being done, but to supply to requests of ourselves here who are testifying—to supply to us details on what steps have been taken, what technology is currently being considered, when has that last been reviewed, and what future technologies are they considering to meet this request, which may require a classified briefing.

Mrs. MILLER. Thank the gentle lady.

The Chairwoman now recognizes——

Ms. RICHARDSON. Did you accept my request?

Mrs. MILLER. Yes. Without objection. Were you concluded? Yes, okay. Without objection, certainly.

Chairwoman now recognizes Ms. Hahn.

Ms. HAHN. Thank you, Madam Chairwoman and Ranking Member. I really am appreciative of this hearing, as I mentioned to you yesterday on the floor. My friend, Congress Member Ted Poe and I have founded the Port Caucus here in Congress.

In December, we actually sent a letter to the chair of the Homeland Security Committee asking for a hearing such as this. I am very pleased that we are holding this.

I have been very interested in the testimony. But I think sitting here this whole time and listening to the question-and-answer, I am not feeling any better about where we are in this country in terms of port security.

I echo many of the comments that my colleague, Ms. Richardson, just made. While neither one of us actually represents the Port of Long Beach or Los Angeles, those two ports, we call them America's ports, because about 44 percent of the trade that comes into this country comes through those port complex.

Both of our districts border those ports. Many of our constituents live minutes from those ports. Any attack, natural or man-made, would be devastating to lives and to the National economy. As Ms. Richardson said, in 2002, we had a labor dispute. Everyone knew it was happening. There was already efforts underway to divert cargo from the West Coast ports.

Yet we were able to determine that it was a $1- to $2-billion-a-day hit to our National economy. It lasted 10 days. So do the math and we know what that did.

Also not to our National economy but the global economy. We heard that many businesses throughout Asia actually were extremely impacted by the loss of cargo moving during that 10 days. Some of the businesses, we even heard, never recovered from that.

So I think the threat to our National economy, the global economy, to lives is severe. I have real concerns. I have always felt like the most vulnerable entryway into this country is through our sea ports. After 9/11, I think we focused in this country, rightly so, on securing our airports.

You know, and we didn't really take into account the costs. We didn't really take into account the inconvenience. I think if the traveling public knew exactly what it was going to entail to make it through security lines, they would have probably balked at what we were recommending.

But we did it because we knew it was important to the safety and security of the traveling public, as well as to our commerce. I don't feel like we have done the same with our ports.

I know there is a lot of vulnerabilities still. I am one of those that would like to see us get to a much greater percentage of scanning. I really think that is imperative.

I think just by your testimony today, you have talked about, you know, really a lot of what you are focusing on is a layered approach, knowing what is in the manifest, believing what is in the manifest, and believing that when it reaches our shores, nothing has happened across the ocean to have tampered with any of that cargo.

Since we have implemented this, I know just at the Port of Los Angeles, there has been twice on the anniversary of 9/11 a National media company actually ship depleted uranium through the port. It was discovered in Los Angeles.

Also know, since we have implemented this, there has been a couple of containers have come in that harbored folks from other countries. One was 19 Chinese in a container, that was discovered by the longshoremen in Los Angeles, not through any of these efforts that are underway.

In terms of costs, you know, the costs that would impact our economy if something were to happen at one of these major ports is significant. But, you know, we were spending, you know, a lot of money on our wars per month. It was $12 billion per month for both of our wars in Iraq and Afghanistan.

We believe that was worth it. We believe that was worth it for the National security. I really think this is at that level. I feel like we are vulnerable.

I think we have all talked about how much we want a greater percentage of screening. I think you have answered where we are at. I think you have heard this warning from a lot of Members of this committee, that we really are interested in seeing you get a higher percentage of scanning.

Let us talk about not when something or if something might happen. Let us talk about when something happens and port disruption. It was touched on in terms of recovering. I know that I am going to be introducing legislation that talks about all of our ports in this country having a recovery plan, because I think that would make our ports less attractive to an attack, if we knew that they could get up and running.

In this Port Caucus, we are going to talk about a recover plan for all of our ports. What would you suggest that we look at, in terms of what would be important for our major ports to get back up in business after a major disruption?

Mr. HEYMAN. Thank you, Congresswoman, for your thoughts on this very important subject. We take this very seriously. We appreciate your seriousness about it as well.

On the resilience and recovery side, it is something that is not as—it has not been as embraced or as thought through as the prevention side. That is because largely we are very concerned about prevention. We have done less on the resilience side.

In the United States, that is why we are taking an initiative and building in resilience internationally in our strategy. In fact, we have led the way, partly through the APAC Forum, of ensuring trade recovery procedures are put in place.

One of the main things that people will do, and frankly, the ports should consider, is having the appropriate information to know where and when things can open, so that businesses can rely on a real understanding of timing and recovery of a disruption.

The sharing of information is one of the things that we can do a lot more on, as it pertains to resilience at these ports.

Ms. HAHN. Let me also ask about once at point of origin, we have got the manifest. It arrived at its point of destination. We are hoping for the best, that nothing has happened on our wide, open seas.

Can any of you speak to that issue? Are you 100 percent sure that when these containers leave their points of origin and when they arrive at their point of destination, nothing has happened? What are we doing to ensure that?

Mr. MCALEENAN. We are trying to make as certain as possible of that. To do that is part of the 10+2 filing. It includes information on where the containers reside on the vessel.

That allows us to see if they might be accessible while they are on the high seas, to determine whether they could be compromised while they are underway. So we do seal checks when they arrive. We are able to compare the seal submitted by the importer and the shipper.

Ms. HAHN. Who does those seal checks?

Mr. MCALEENAN. U.S. Customs and Border Protection, usually officers at the port of entry. So, in other words, this is a concern. It is something we take seriously. We work with our partners in the Coast Guard as the vessels approach the U.S. ports.

But——

Ms. HAHN. Do you seal checks on all the containers?

Mr. MCALEENAN. No. We do targeted seal checks and also random operations to ensure the integrity.

Ms. HAHN. See, and that is what makes me nervous too, again. It keeps me up at night, is that random, you know, your kind of best guess on where to even check the seals.

You know, as more and more of our ports are going to go automated, I am concerned that the loading and unloading of our cargo by automation, as opposed to real folks, I think presents a bit of a risk.

Thank you.

Mrs. MILLER. I want to thank the—turn my mike on. I certainly want to thank all the participation from the Members today. It has been I think one of our—well, we have had some great hearings, but this certainly has been a good one, I think a lively one, a good discussion.

I certainly want to thank all of the witnesses for your testimony. I sincerely want to thank you all for your service to our Nation. I know I speak on behalf of all of the Members, as we are obviously working in an extremely bipartisan fashion about National security.

My staff gets sick of me saying this, but I say it all the time and try to remind certainly myself that with all the issues that the Congress faces, the first and foremost responsibility of the Federal Government is provide for the common defense.

That is actually in the preamble of our Constitution. So National security, homeland security, all of these kinds of things are always our priority.

So it has been very eye-opening to hear about some of the dollars that would be involved in us getting to where we may want to get to. I think you can see, again from a bipartisan standpoint, that we are very cognizant of the challenges to ever get to 100 percent, whether or not it is even feasible.

That is why we have been waiting for the Secretary to come forward with possibly some legislation to modify the current mandate or what have you. But this subcommittee is very, very interested

in assisting you with the resources that you all need to do your jobs, and the mission that we have tasked you with.

You are out there every single day. It really is for us, as I say, to prioritize our spending here. Again, I will say that from a bipartisan standpoint, because it is interesting hearing that the administration is proposing a 50 percent reduction in the CSI program.

But yet I certainly understand the makeup of all of that as well. It is expensive to have officers overseas, et cetera. So we are not looking for a sound bite here. We really are trying to understand how we prioritize our spending and do what we need to do to keep our Nation safe, particularly through our ports.

So again, I appreciate all of the witnesses, your testimony. With that, I would mention also that the hearing record will be open for 10 days. If there is any additional questions, we all may submit those as well.

Without objection, subcommittee stands adjourned. Thank you very much.

[Whereupon, at 12:01 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FOR DAVID HEYMAN FROM CHAIRWOMAN CANDICE S. MILLER

Question 1. Secretary Napolitano has stated that the 9/11 Act's mandate to scan 100% of maritime cargo containers is not achievable, does not necessarily make sense, and is not in line with the current risk-based approach. In fact, the Secretary has stated that the "mandate was constructed at a time before we had really a mature understanding of what that meant."

What is the current status of the DHS efforts to meet the 100% scanning mandate?

Answer. DHS remains committed to ensuring that all goods coming into the United States are secure and do not pose a threat to our citizens or National interests. This is an area where we have done a significant amount of work, particularly with regard to containerized maritime cargo where we see such huge volumes of goods arriving each year. The SAFE Port Act required DHS to implement a pilot program to assess the feasibility and potential challenges with a 100 percent maritime container scanning program, titled the Secure Freight Initiative, or "SFI." SFI was deployed in six international ports in 2007 and 2008, double the required number. It demonstrated to us both the value that scanning can provide but also the significant impacts and challenges such a regime can pose if not implemented thoughtfully. As outlined in six annual reports to Congress titled Update on Integrated Scanning System Operations, these challenges included cargo processing delays, limited space within ports for the systems, high costs, diplomatic issues, and immature technologies. In light of these challenges, five of the six pilot project locations have reverted to Container Security Initiative (CSI) protocols of risk-based targeting and only the Port of Qasim in Pakistan remains an active SFI location.

Question 2. Why was the 100% scanning mandate not addressed within the recently released Global Supply Chain Security Strategy?

Answer. The National Strategy for Global Supply Chain Security (Strategy) does not address any specific statutes, programs, or initiatives, including the 100 percent maritime containerized cargo provision. Instead, the Strategy provides a high-level, integrated vision on a broad and complex topic. It establishes a collaborative risk-based approach to pursuing our goals of security, efficiency, and resiliency in the global supply chain. As a number of recent threats have shown us, the global supply chain is dynamic, growing in complexity and size, and remains vulnerable to a host of threats and hazards. A common approach is necessary to strengthen and protect this vital system. The Strategy is an important first step; it will enhance coordination among the many U.S. departments and agencies with responsibilities related to the global supply chain and convey our goals and priorities to stakeholders interested in collaborating with us.

Question 3. Does DHS intend to move forward with implementing the 100% scanning mandate?

Answer. At this time, DHS is assessing whether it will be necessary to extend the deadline for the 100% scanning mandate established in Section 232(a) of the SAFE Port Act. We currently believe that at least three of the conditions for a 2-year extension exist but our assessment is not yet complete, nor has a final decision been made.

While no decision has been made yet on the extension, the National Strategy for Global Supply Chain Security does identify promoting necessary legislation that supports implementation by Federal departments and agencies. Should a determination be made to pursue amending the mandate to reflect the Strategy's layered, risk-based approach, DHS would seek to work with Congress.

In the mean time, we continue to work in concert with other departments and agencies (such as the Departments of Energy, Defense, Commerce, and State) to ensure that our Nation's nuclear non-proliferation programs remain strong and global security measures to combat this threat are advanced.

Question 4. Is 100% scanning an achievable goal?

Answer. We do not believe that 100 percent scanning is an achievable goal, given the challenges previously noted. We are and continue to be committed to using a risk-based security approach and multiple layers of defense. We will continue work with Congress to refine our approach and ensure that scanning remains a key layer of our risk-based security system.

Question 5. If 100% scanning were fully implemented, what would the initial and on-going costs to the Federal Government be to establish, maintain, and operate such a regime?

Answer. DHS estimates that fully implementing the 100 percent scanning mandate would require establishing 2,100 scanning lanes across approximately 700 ports worldwide. A conservative estimate, based on costs associated with the Secure Freight Initiative pilots, is that such an effort would cost $16.8 billion dollars. This estimate does not factor the impacts and costs to the shipping industries or an estimated $2.9 billion annual operations and maintenance of the scanning equipment. If the 100 percent scanning mandate were fully implemented using currently available technological systems, the trade capacity impact on the flow of cargo would be significant.

QUESTIONS FOR DAVID HEYMAN FROM HONORABLE MIKE ROGERS

Question 1. TSA and the Coast Guard completed the Transportation Worker Identification Credential (TWIC) reader pilot program in May 2011. DHS has failed to publish their assessment regarding the pilot program, even though the Coast Guard Authorization Act of 2010 specifically required these findings to be submitted to Congress within 4 months of the completion of the program. Furthermore, the failure to complete this report has delayed the publication of the TWIC reader regulations, and now DHS does not expect to publish this key rulemaking until July 2012 at the earliest.

What is the status of the Department's findings on the TWIC reader pilot program?

Answer. The Transportation Worker Identification Credential Reader Pilot Report was signed by the Secretary on February 27, 2012, and delivered to the following committees: The Senate Committee on Commerce, Science, and Transportation, the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Homeland Security, and the House Transportation and Infrastructure Committee.

Question 2. Why is this report already over 4 months late, and Congress still has yet to receive it?

Answer. The Transportation Worker Identification Credential Reader Pilot Report underwent a thorough review by a number of components within DHS prior to the Secretary's approval.

Question 3. When can we expect to have this report?

Answer. The Transportation Worker Identification Credential Reader Pilot Report was delivered to the required House and Senate Committees on February 27, 2012.

Question 4. When can we expect the TWIC reader regulations to be published?

Answer. The Coast Guard is working diligently to publish the TWIC Reader Notice of Proposed Rulemaking (NPRM). An Advanced Notice of Proposed Rulemaking (ANPRM) on the TWIC reader requirements was published in the *Federal Register* on March 27, 2009. The ANPRM comments have been analyzed along with pilot data, and together they will help inform the Notice of Proposed Rulemaking (NPRM). It is difficult to predict when the final TWIC reader requirements might be implemented, as the Coast Guard is required to review, analyze, and take public comments into account before any final TWIC reader requirements can be implemented. For this reason, the Coast Guard does not have a precise date for publication of the TWIC reader rulemaking project.

QUESTIONS FOR PAUL F. ZUKUNFT FROM HONORABLE MIKE ROGERS

Question 1. TSA and the Coast Guard completed the Transportation Worker Identification Credential (TWIC) reader pilot program in May 2011. DHS has failed to publish their assessment regarding the pilot program, even though the Coast Guard Authorization Act of 2010 specifically required these findings to be submitted to Congress within 4 months of the completion of the program. Furthermore, the failure to complete this report has delayed the publication of the TWIC reader regulations, and now DHS does not expect to publish this key rulemaking until July 2012 at the earliest.

What is the status of the Department's findings on the TWIC reader pilot program?

Answer. The Transportation Worker Identification Credential Reader Pilot Report was signed by the Secretary on February 27, 2012, and delivered to the following committees: The Senate Committee on Commerce, Science, and Transportation, the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Homeland Security, and the House Transportation and Infrastructure Committee.

Question 2. Why is this report already over 4 months late, and Congress still has yet to receive it?

Answer. The Transportation Worker Identification Credential Reader Pilot Report underwent a thorough review by a number of components within DHS prior to the Secretary's approval.

Question 3. When can we expect to have this report?

Answer. The Transportation Worker Identification Credential Reader Pilot Report was delivered to the required House and Senate Committees on February 27, 2012.

Question 4. When can we expect the TWIC reader regulations to be published?

Answer. The Coast Guard is working diligently to publish the TWIC Reader Notice of Proposed Rulemaking (NPRM). An Advanced Notice of Proposed Rulemaking (ANPRM) on the TWIC reader requirements was published in the *Federal Register* on March 27, 2009. The ANPRM comments have been analyzed along with pilot data, and together they will help inform the Notice of Proposed Rulemaking (NPRM). It is difficult to predict when the final TWIC reader requirements might be implemented, as the Coast Guard is required to review, analyze, and take public comments into account before any final TWIC reader requirements can be implemented. For this reason, the Coast Guard does not have a precise date for publication of the TWIC reader rulemaking project.

QUESTIONS FOR KEVIN K. MCALEENAN FROM CHAIRWOMAN CANDICE S. MILLER

Question 1. At the Border and Maritime Security Subcommittee hearing focusing on Supply Chain Security held on February 7, 2012, you testified that CBP has concluded that implementing 100% scanning could cost more than $16.8 billion.

Please breakdown this number and explain this $16.8 billion cost.

Answer. DHS estimates that fully implementing the 100 percent scanning mandate would require establishing 2,100 scanning lanes across approximately 700 ports worldwide. A conservative estimate, based on costs associated with the Secure Freight Initiative pilots, is that such an effort would cost $16.8 billion dollars. This estimate does not factor the impacts and costs to the shipping industries or an estimated $2.9 billion annual operations and maintenance of the scanning equipment.

To develop this estimate, CBP first assessed the costs associated with operations at the Container Security Initiative (CSI) ports as well as the Secure Freight Initiative pilots. CBP determined that 187 suites of technology were used to maintain operations at the 58 CSI ports and 12 additional locations. The costs associated with these 187 suites of technology are broken down further below.

- Non-Intrusive Inspection Systems
  - $3.5 million–$4.5 million each
  - Total cost for 187 units is between $654 million–$841 million
- Radiation Portal Monitor Systems
  - $400,000 each
  - Total cost for 187 units is approximately $74.8 million
- Information Technology Transmission
  - $800,000
  - Total cost for supporting 187 units is $149.6 million
- Construction
  - $1 million per site
  - Total costs for all 187 suites is $187 million
- Staffing
  - $500,000 per officer
  - Total cost for 2–4 officers required per port is $187 million–$374 million
- Approximate total for 187 suites of technology needed to support the 58 CSI ports and additional 12 pilot locations was therefore $1.25 billion–$1.62 billion

We arrived at the total implementation estimated cost of $16.8 billion by extrapolating the costs above associated with the 70 locations to the more than 700 ports (2,100 lanes) that shipped maritime containers to the United States in 2009 (the year the analysis was conducted).

Question 2. Is this $16.8 billion the initial start-up cost, and if so, what are the annual reoccurring costs for implementing 100% scanning?

Answer. $16.8 billion is the start-up cost for 700 ports and the annual operations and maintenance costs would be approximately $2.9 billion.

Question 3. Please explain how you came up with this figure and provide any documentation that supports the $16.8 billion cost.

Answer. In fiscal year 2009 (the year the analysis was completed) there were approximately 700 ports that shipped cargo to the United States. We used the analysis from 70 ports (58 CSI ports and 12 additional ports) to estimate of the number of suites of technology required for those 70 ports to implement 100 percent scanning. Based on the additional ports shipping to the United States and the volume of cargo from each of those ports, CBP estimated that it would require approximately 2,100 suites of technology for all ports to implement 100 percent scanning. CBP used a figure of approximately $8 million per suite of technology for a total of approximately $16.8 billion. This does not include the cost to the trade if they were charged for scanning or if containers were delayed.

Question 4. In the Secretary's recent State of the Homeland Address, she explained the rationale behind a risk-based approach to Homeland Security and expounded on the need for strong partnerships with industry, foreign governments, and other key stakeholders. One program that incorporates cooperation with industry to provide additional layers of security in exchange for certain benefits is the C–TPAT program. While C–TPAT has been a largely positive program, it does have several limitations. Some participants in the voluntary program have complained that they are not realizing certain privileges of membership.

What are you doing to increase participation in C–TPAT? Are you considering new or additional benefits for some or all members?

Answer. Tiered Benefit Levels for importer partners ensure that examination benefits are commensurate with the partner's status in the program and are recognized by the Security and Accountability for Every (SAFE) Port Act. The highest level of program benefits are awarded to those partners that exceed the minimum-security criteria through innovation and dedication to excellence.

The program is currently surveying members requesting input on additional benefits.

C–TPAT is in the process of implementing a National standard operating procedures to ensure for front-of-the-line benefits at ports of entry.

C–TPAT is looking into areas for program expansion which would include critical nodes in the international supply that may not require a large commitment of current limited resources to physically visit. One possibility is to expand the Foreign Manufacturer sector (which is currently limited to those companies which qualify in Mexico and Canada) to allow for global participation. Many of the companies who would qualify have been visited at least once already by C–TPAT teams as part of validations of U.S. importer supply chains and could in many cases be validated based on previous visit(s) data. Furthermore, many of these companies are participants in AEO programs which C–TPAT has established Mutual Recognition Arrangements with and could potentially validate based on the AEO visit data. Similar potential may exist in the foreign-based consolidator sector where these facilities are often visited as part of U.S. importer validations. Historical data could be leveraged to increase membership while minimizing the impact on operational resources because initially, many new companies in the previously described examples could be virtually validated (not requiring physical trips).

Question 5. What have been some of the biggest impediments to further expanding the C–TPAT program?

Answer. CBP has carefully expanded the program since its inception to include new entities which have the physical means to enhance security along these critical points. In accordance with the SAFE Port Act of 2006, CBP established new membership communities for Mexican Long Haul Carriers, Foreign Marine Port Terminal Operators by invitation, and third party logistics providers. The decision to expand C–TPAT membership to include these groups was made in close consultation with the trade community including the U.S. Department of Homeland Security's Commercial Operations Advisory Committee.

Existing members have expressed concern with a possible softened posture on eligibility requirements that would imply that new members will be subjected to a less robust validation process.

Question 6. I understand that each C–TPAT supply chain specialist is responsible for about 75 companies. Have staffing shortages limited the expansion or effectiveness of the C–TPAT program?

Answer. Our current staffing levels are adequate to meet our existing workload. However, human capital and funding will need to grow at a commensurate rate as the program expands in order to manage the increase in vetting, validation process, and C–TPAT partner account maintenance.

Question 7. What steps has the Department taken to link with our foreign partners and improve the security of the entire global supply chain in terms of aligning

our trusted shipper program, C–TPAT, with similar and effective programs abroad, such as Europe's AEO program or Canada's PIP program?

Answer. CBP continues to collaborate with foreign customs administrations to improve efficiency and reduce redundancy within their respective trusted trader programs. Mutual Recognition (MR) links the various international industry partnership programs so that they create a unified and sustainable global security posture. CBP has signed MR Arrangements with five countries and is also working with three additional entities towards MR (Taiwan, Singapore, and the European Union).

Mutual Recognition countries:

New Zealand—Secure Export Scheme (SES) (MR signed in June 2007)

- Observe New Zealand validation visits in accordance with MRA.

Canada (MR signed in June 2008)

- PIP and C–TPAT have jointly developed single application requirements for highway carriers and conducted a pilot with 4 highway carrier companies (2 located in Canada and 2 in the United States) in the first quarter of 2011. The joint pilot was successful and illustrated the feasibility of the single application with single entity to single entity.

Jordan—Golden List (MR signed in June 2008)

- Increase communication with Jordan's Golden List program to improve Mutual Recognition.

Japan AEO (MR signed in 2009)

- Continue open communication and implementation of Mutual Recognition.
- Conduct Export pilot for C–TPAT companies that export to Japan in 2012.
- In accordance with the MRA signed, observed their validation process in December 2011.

South Korea AEO (MR signed in June 2010)

- Continue open communication and implementation of Mutual Recognition
- In accordance with the MRA signed, observed their validation process in December 2011.

Future MR Arrangements:

EU AEO

- Finalize Mutual Recognition Arrangement and implement reciprocal benefits.
- Accepting MRA certificates from the European Union for foreign manufacturers in lieu of visiting the foreign site.
- Mutual Recognition Arrangements with the European Union is expected to be signed on May 4, 2012. Implementation to follow soon afterwards.

Taiwan AEO

- In February 2012, conducted joint validation visits towards signing a Mutual Recognition Agreement, implement reciprocal benefits by 2012.
- Taiwan AEO will be observing C–TPAT Validations in the United States the week of April 23, 2012.

Singapore—Secure Trade Partnership (STP)

- In March 2012, conducted joint validation visits towards signing a Mutual Recognition Agreement, implement reciprocal benefits by 2012.
- Singapore STP will be observing C–TPAT Validations in the United States the week of June 4, 2012.
- C–TPAT HQ and International Affairs will be meeting with Singapore STP representative the week of June 11, 2012 in Washington, DC.

CBP is also actively engaged with other countries' Authorized Economic Operator (AEO) programs to improve the security of the international supply chain:

Mexico AEO

- Continue to work with Mexican Customs AEO program Nuevo Esquema de Empresas Cerificadas (NEEC) to provide technical assistance and further advance supply chains originating in Mexico. C–TPAT and NEEC developed a strategy to recognize C–TPAT manufacturers into Mexico's program. The objective of this strategy is to increase NEEC membership giving it instant credibility; and to help both programs synchronize procedures and standards to ensure maximum compatibility. This will eventually facilitate the road towards mutual recognition between the United States and Mexico. So far, 295 C–TPAT manufacturers operating in Mexico have agreed to join the NEEC program.

Colombia

- Conduct Export Pilot for C–TPAT companies that export to Colombia in 2012. Companies in both the United States and Colombia have been identified and invited to participate in the pilot. Colombia's program remains young and it will need sometime to process the applications and eventually certifiy the companies that will be participating in this pilot program.

China
- Continue open communication and joint validations, with the possibility of Mutual Recognition Agreement.

Costa Rica Programa de Facilitacion Aduanera para el Comercio Confiable en Costa Rica PROFAC (Customs Facilitation Program for Trusted Trade in Costa Rica)
- Costa Rican AEO program PROFAC has identified their four Export Pilot companies to participate in the pilot program. Maria Iris Cespedes will e-mail Bryan Picado with names and MID numbers. She also expressed that she would like to include an additional company as back-up.
- Deliverables and a time line have been established to launch the "Export Pilot Program" by August 2012. PROFAC has recruited five companies which are in the process of applying.
  - April 23–30, PROFAC will determine if companies are eligible to participate in Export Pilot Program via a self-evaluation questionnaire provided by PROFAC.
  - May–July, all eligible companies will be certified via PROFAC's internal vetting process and validated jointly by PROFAC and C–TPAT to ensure a side-by-side comparison of C–TPAT's minimum security criteria.
  - Once all eligible companies successfully pass vetting and are in compliance with PROFAC and C–TPAT's minimum security criteria, the "Export Pilot Program" will be launched in the month of August

Guatemala AEO
- Continue cooperative efforts and provide training and assistance.

Dominican Republic
- Continue cooperative efforts and provide training and assistance.

Turkey AEO
- Continue cooperative efforts and provide training and assistance.

India AEO
- Continue cooperative efforts and provide training and assistance.

Brazil AEO
- Continue cooperative efforts and provide training and assistance.

Question 8. What concerns do you have about such mutual recognition agreements?

Answer. C–TPAT receives requests from foreign governments for assistance and capacity-building on trusted trader/mutual recognition programs. The program is concerned with meeting ever-increasing requests for MRA capacity-building due to our limited staff resources.

Question 9. Has there been any consideration of including third-party logistic providers in the C–TPAT program?

Answer. Currently, C–TPAT is considering the inclusion of asset-based warehouses that are located within close proximity or equivalent of the port of arrival that receive international cargo directly from the port in excess of 500 Twenty-Foot Equivalent Units (TEUs). The value of adding this sector is that these entities are the "first domestic custodians" to verify the integrity and number of the seal and reconcile the cargo against the manifest.

The decision to create a new entity in the program takes into account several factors, including the ability of participating businesses to physically influence security practices and procedures abroad, available program resources, and redundancy with other existing security programs. In developing the eligibility criteria for the third-party logistic providers' (3PLs') sector, CBP determined that non-asset-based 3PLs which perform duties such as quoting, booking, routing, and auditing, but which do not own warehousing facilities, vehicles, aircraft, or any other transportation assets, should be excluded from C–TPAT enrollment. As these type of 3PLs may possess only desks, computers, and freight industry expertise, such entities would have limited ability to exert influence on their business partners in the international supply chain. CBP does not believe it would be prudent to use its limited program resources to validate such entities, most of which are based solely in the United States, when resources would be better served to validate entities abroad.

QUESTIONS FOR STEPHEN L. CALDWELL FROM CHAIRWOMAN CANDICE S. MILLER[1]

Question 1. GAO has completed extensive work regarding the C–TPAT program. Has the C–TPAT program been effective in accomplishing its goal of encouraging companies to boost their security programs?

[1] [sic]

On the basis of work we performed as part of our last review of the Customs-Trade Partnership Against Terrorism (C–TPAT) program in April 2008,[2] as well as more recent follow-up work we performed to determine the status of our recommendations from that report, we believe that U.S. Customs and Border Protection (CBP) has been successful in getting companies to join C–TPAT and verifying that the member companies are generally following minimum standards designed to improve their security.[3] Specifically, as part of our 2008 C–TPAT review, we assessed the progress CBP had made in addressing challenges in validating C–TPAT members' security practices, among other things. We reported that CBP had introduced a process to award benefits for C–TPAT importers depending on validation of their security practices, and that CBP had taken steps to improve the security validation process, but faced challenges in verifying that C–TPAT members' security practices meet minimum criteria. For example, we found in 2008 that CBP lacked a systematic process to ensure C–TPAT members take appropriate actions in response to CBP security specialists' recommendations during validation inspections. Without such a key internal control, CBP did not have reasonable assurance that companies would implement its recommendations to enhance supply chain security practices in accordance with CBP criteria. In response to recommendations we made in our April 2008 report, CBP has taken a number of actions to strengthen the C–TPAT program and better ensure its process for validating C–TPAT members' security procedures.

To address the challenges noted in the report related to verifying that C–TPAT members' security practices meet minimum criteria, we recommended that, among other things, CBP strengthen the evaluation of members' security practices by requiring that validations include the review and assessment of any available results from audits, inspections, or other reviews of a member's supply chain security. CBP has addressed this and other recommendations from our 2008 review. For example, CBP issued policy guidance in May and June 2008, shortly after our report was issued, that instructs field directors and supervisors to immediately require supply chain specialists to: (1) Request information from C–TPAT members about any audits or inspections conducted of its security practices as part of preparing for the validation visit and (2) ensure any required actions and recommendations from C–TPAT validation reports are completed. Further, in response to a separate GAO recommendation, CBP has explored options for developing performance measures to assess the effectiveness of the C–TPAT program in enhancing supply chain security.

Question 2. Do you think that companies are properly incentivized to join C–TPAT? Have the benefits CBP promises to C–TPAT members been fully realized?

Answer. C–TPAT membership has increased over time, indicating an incentive for companies to participate in the program. Specifically, at the end of 2007, CBP had initially certified fewer than 8,000 members, and by November 2010 CBP had certified over 10,000 members. While we have not conducted work to specifically evaluate the incentives or benefits of the C–TPAT program, according to CBP, some of the benefits of participating in C–TPAT include improved predictability in moving goods and services, decreases in supply chain disruptions, and reductions in cargo theft and pilferage. Further, according to CBP, C–TPAT importers are 4 to 6 times less likely to incur a security or compliance examination. However, as we reported in October 2009, the incentives to join C–TPAT could diminish with the implementation of 100 percent scanning because C–TPAT members would not receive the benefit of fewer examinations.[4] According to a survey conducted in 2007 by the University of Virginia, the most important motivation for businesses joining C–TPAT was reducing the time and cost of cargo getting released by CBP.[5] This benefit could be diminished by the 100 percent scanning requirement, though, since under such a requirement all cargo is to be scanned regardless of C–TPAT membership. This view was shared by 3 of the 6 C–TPAT members we interviewed for our October 2009 report who stated that there would be less incentive to maintain membership or for

---

[2] 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, DC: Apr. 25, 2008).

[3] The DHS Inspector General (DHS–IG) is currently conducting an audit of the C–TPAT program to determine the extent to which CBP ensures that highway carriers participating in the program have implemented security measures that meet the minimum security requirements of C–TPAT. The DHS–IG expects to issue the report on the results of this review at the end of April 2012.

[4] GAO, *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, DC: Oct. 30, 2009).

[5] University of Virginia, *Customs-Trade Partnership Against Terrorism (C–TPAT) Cost/Benefit Survey* (August 2007).

other companies to join C–TPAT if the 100 percent scanning requirement were fully implemented.

Question 3. In your research, has CBP been able to hold C–TPAT members accountable for their security procedures? Is the C–TPAT validations process working?

Answer. As part of the program, CBP requires C–TPAT members to submit plans for their security measures, and to hold members accountable, CBP conducts a validation to ensure that members have implemented the security measures as planned. In conducting a validation, CBP may make recommendations for improvement. In some cases, CBP has determined that the security measures have not been implemented and has suspended or removed companies from the program.

Since we completed our last review of the C–TPAT program in 2008, we do not have current information regarding how the validations process is working. However, based on monitoring we have conducted of the program since we issued our report, we have verified that CBP has taken a number of actions to strengthen the C–TPAT program and better ensure its process for validating C–TPAT members' security procedures. In response to our recommendations, CBP made changes to its records management system to automatically document time-sensitive decisions mandated by the Security and Accountability For Every (SAFE) Port Act.[6] At the time of our follow-up in October 2009, CBP demonstrated that its system tracked 90-day certification, validation within 1 year of a company being certified, and re-validation within 3 years of the initial validation. According to CBP's fiscal year 2013 budget request, CBP is planning to extend the re-validation cycle from 3 years to 4 years in an effort to save $5 million in fiscal year 2013. The impact that this potential change will have on C–TPAT members' security practices is unknown.

Question 4. In your testimony, you note that GAO has recommended saving Government funds by migrating the Container Security Initiative (CSI) to a more remote-screening system based upon reciprocity agreements with foreign partners.

How much money has CBP saved by moving screening personnel back to America?

Answer. CBP has saved approximately $35.4 million cumulatively over fiscal years 2010 and 2011 as a result of the changes to its staffing model, which included transferring Container Security Initiative (CSI) positions from overseas to the National Targeting Center—Cargo in the United States. We recommended in April 2005 that CBP revise the CSI staffing model to consider what functions needed to be performed at overseas CSI ports and what functions could be performed remotely in the United States.[7] In response to our recommendation, CBP issued a human capital plan in May 2006 that did not specify that CSI targeting positions be located at CSI seaports, thus recognizing that officers could support CSI ports from the National Targeting Center—Cargo in the United States.

Question 5. Could CBP move further with this initiative and move even more of their personnel back to America and migrate the CSI program to a more reciprocity-based system? Would this save additional taxpayer dollars?

Answer. Relocating additional CSI positions from overseas ports to the United States could result in cost savings; however, according to CBP officials, it could also affect how the CSI program works and its effectiveness. According to CBP officials, cost savings may be realized in expenses, such as housing, by moving certain CSI functions and positions back to the United States, but some costs (such as office space and communications equipment) would not be eliminated entirely unless CBP removed all officers stationed at each foreign port. According to CBP officials, if CBP were to relocate its officers from all CSI ports, one of the primary methods for ensuring the effectiveness of CSI operations, namely the working relationships between CBP targeters and host government officials, would also be eliminated. In visiting ports as part of work issued in January 2008, we observed that relationships with host governments have improved over time, leading to increased information sharing between governments and a bolstering of host government customs and port security practices, among other things.[8] CBP officials also explained that if there are no CBP officers stationed at a foreign port, CBP would have to rely more heavily on foreign governments' cooperation in conducting cargo examinations, which would require negotiations with the host governments before changing the operations at the port, and this could be a difficult and time-consuming process. According to CBP

---

[6] Pub. L. No. 109–347, 120 Stat. 1884 (2006).

[7] GAO, *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts,* GAO–05–557 (Washington, DC: Apr. 26, 2005).

[8] 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, DC: Jan. 25, 2008).

officials, CBP plans to fill some existing vacancies in overseas CSI positions, and upon filling those positions it plans to maintain its level of overseas staffing for the CSI program. These officials also explained that CBP has no significant changes planned for the program, such as expanding or reducing the number of participating ports.

Question 6. In your testimony, you mentioned two programs where CBP spent significant sums and then canceled the programs with little to show in the way of achievements. You specifically note that the DHS spent $200 million developing a new advanced spectroscopic portal (ASP), but then canceled the program before updating their cost-benefit analysis. In addition, DHS spent $113 million on the cargo advanced automated radiography system (CAARS) and then canceled the program.

What happened here? Why were such vast sums expended on this new technology and then DHS turned away from these ideas? How can we prevent this type of waste in the future?

Answer. To prevent these types of situations from recurring in the future, we reported in September 2010 that DHS should consider incorporating lessons learned, identified by our reviews of the ASP and CAARS programs, in its continuing efforts to develop technology for detecting nuclear materials in vehicles and containers at U.S. ports of entry. These lessons learned included: (1) Enhancing interagency collaboration and coordination, (2) engaging in a robust Departmental oversight review process, (3) separating the research and development functions from acquisition functions, (4) determining the technological readiness levels before moving forward to acquisition, and (5) rigorously testing devices using actual agency operational tactics before making acquisition decisions. In addition, we are engaged in on-going work reviewing the results of ASP testing conducted after our last report on the ASP program in 2009. As part of this on-going work, we will identify lessons learned from the ASP testing campaign. We expect to report on the results of this work by the end of 2012.[9]

Regarding the ASPs, we reported in June 2009 that many major DHS investments, including the ASP program, had not met the Department's requirements for basic acquisition documents necessary to inform the investment review process. As a result, DHS had not consistently provided the oversight needed to identify and address cost, schedule, and performance problems in its major investments.[10] Moreover, emphasizing expediency in replacing existing equipment with new portal monitors led to an ASP testing program that initially lacked the necessary rigor. Additionally, we reported that DHS's decision to replace existing equipment with the ASPs was not justified due to the marginal improvement offered by the new technology and the potential to improve the current-generation portal monitors' sensitivity to nuclear materials, most likely at a lower cost. For example, though preliminary test results showed that ASPs performed better than current-generation portal monitors in detecting certain weapons-usable nuclear materials concealed by light shielding, as approximated by the Department of Energy's threat guidance, differences in sensitivity were less notable when shielding was slightly below or above that level. We also reported in November 2009 that the ASPs experienced serious problems during testing.[11] For example, the ASPs had an unacceptably high number of false positive alarms for the detection of certain high-risk nuclear materials. In addition, ASPs experienced a "critical failure," which caused an ASP to shut down. Importantly, during this critical failure, the ASP did not alert the CBP officer that it had shut down and was no longer scanning cargo. As a result, were this not in a controlled testing environment, the CBP officer would have permitted the cargo to enter the country thinking the cargo had been scanned, when it had not. Finally, the Director of DHS's Domestic Nuclear Detection Office (DNDO) indicated during a July 2011 hearing that the speed of trucks passing through the ASP was an additional problem and contributed to DNDO's decision to cancel the ASP program as originally conceived.

Regarding CAARS, in September 2010, we reported that DHS's decision to cancel acquisition of the CAARS program in December 2007 was due to the system's inability to satisfy operating requirements at ports of entry coupled with technological shortcomings. Officials from DNDO and the system's end-user, CBP, acknowledged

---

[9] We are conducting this work for the Ranking Members of the Subcommittee on Investigations and Oversight and Subcommittee on Energy and Environment; Committee on Science, Space, and Technology; House of Representatives.

[10] GAO, *Combating Nuclear Smuggling: Lessons Learned from DHS Testing of Advanced Radiation Detection Portal Monitors,* GAO–09–804T (Washington, DC: June 25, 2009).

[11] GAO, *Combating Nuclear Smuggling: Recent Testing Raises Issues About the Potential Effectiveness of Advanced Radiation Detection Portal Monitors,* GAO–10–252T (Washington, DC: Nov. 17, 2009).

that they had few discussions regarding operating requirements at ports of entry during the first year or more of the program. As a result, DNDO pursued the acquisition and deployment of CAARS machines without fully understanding that they would not fit within existing primary inspection lanes at CBP ports of entry. In addition, regarding CAARS technology, the development of the system's algorithms (software)—a key component needed to identify shielded nuclear materials automatically—did not mature at a rapid enough pace to warrant acquisition and deployment.

QUESTIONS FOR STEPHEN L. CALDWELL FROM HONORABLE MIKE ROGERS

Question 1. GAO has done extensive work to review and test the Transportation Worker Identification Credential (TWIC) program.

What do you see as the major deficiencies in the program?

Answer. As discussed in our May 2011 report, the TWIC program faces several challenges in meeting its mission needs.[12] We reported that internal control weaknesses governing the enrollment, background checks, and use of TWIC potentially limit the program's ability to provide reasonable assurance that access to secure areas of Maritime Transportation Security Act (MTSA)-regulated facilities is restricted to qualified individuals. Key program weaknesses included an inability to provide reasonable assurance that only qualified individuals can acquire TWICs or that once issued a TWIC, TWIC-holders have continued to meet eligibility requirements. Moreover, internal control weaknesses in TWIC enrollment, background checks, and use could have contributed to the breach of MTSA-regulated facilities during covert tests conducted by GAO's investigators.

Question 2. Do you think that getting the regulations on TWIC readers pushed out of the Department and getting these readers installed in our ports will help rectify some of these deficiencies?

Answer. Implementation of a card reader system will not address the enrollment, background checks, and deployment weaknesses we identified in our May 2011 report. These weaknesses could render the electronic reader check moot, by allowing unqualified individuals to acquire authentic TWICs using a counterfeit identity and then using the TWICs for accessing MTSA-regulated facilities and vessels using electronic card readers.[13] If an individual presents an authentic TWIC acquired through fraudulent means when requesting access to the secure areas of a MTSA-regulated facility or vessel, the cardholder is presumed to have met TWIC-related qualifications during a background check. Further, the extent to which the use of TWIC readers will help identify the use of counterfeit TWICs (that is, TWICs produced independently by individuals seeking to circumvent port security) at MTSA-regulated facilities and vessels will largely depend on how each card reader system is implemented in practice. The ability of readers to identify counterfeit TWICs depends on the sophistication of the counterfeit and the mode that the reader is set to when reading a TWIC. There are four mode settings. Each increasing mode requires a longer time to read the TWIC but also provides greater assurance that the TWIC is authentic and belongs to the person that is presenting it. Consequently, there is a tradeoff between throughput and security. For example, at lower settings/modes the reader is not comparing the cardholder's fingerprint to the fingerprint stored on the card, but the card is read faster than when the reader is set to read the fingerprint. We recommended that DHS perform an internal control assessment of the TWIC program by: (1) Analyzing existing controls, (2) identifying related weaknesses and risks, and (3) determining cost-effective actions needed to correct or compensate for those weaknesses so that reasonable assurance of meeting TWIC program objectives can be achieved.

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

[13] In commenting on our May 2011 report, DHS stated that document fraud is a vulnerability to credential-issuance programs across the Federal Government, State and local governments, and the private sector.