S. HRG. 111–516

TRANSPORTATION CHALLENGES AND CYBERSECURITY POST-9/11

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

DECEMBER 2, 2009

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

U.S. GOVERNMENT PRINTING OFFICE

55–979 PDF WASHINGTON : 2010

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

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

DANIEL K. INOUYE, Hawaii
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
MARK PRYOR, Arkansas
CLAIRE MCCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
TOM UDALL, New Mexico
MARK WARNER, Virginia
MARK BEGICH, Alaska

KAY BAILEY HUTCHISON, Texas, *Ranking*
OLYMPIA J. SNOWE, Maine
JOHN ENSIGN, Nevada
JIM DEMINT, South Carolina
JOHN THUNE, South Dakota
ROGER F. WICKER, Mississippi
GEORGE S. LEMIEUX, Florida
JOHNNY ISAKSON, Georgia
DAVID VITTER, Louisiana
SAM BROWNBACK, Kansas
MIKE JOHANNS, Nebraska

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
BRUCE H. ANDREWS, *General Counsel*
ANN BEGEMAN, *Acting Republican Staff Director*
NICK ROSSI, *Republican Chief Counsel*
BRIAN M. HENDRICKS, *Republican General Counsel*

CONTENTS

WITNESSES

APPENDIX

TRANSPORTATION CHALLENGES AND CYBERSECURITY POST-9/11

WEDNESDAY, DECEMBER 2, 2009

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

The Committee met, pursuant to notice, at 10 a.m. in room SR–253, Russell Senate Office Building, Hon. John D. Rockefeller IV, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

The CHAIRMAN. Madam Secretary, people are coming, I promise. And it's just—every day is one of those days, right?

Secretary NAPOLITANO. I hear you.

The CHAIRMAN. You know a little bit about that.

Secretary NAPOLITANO. I do, indeed.

The CHAIRMAN. The—one of the things I wanted to make, which is not in my statement, that Commerce Committee is—we're really glad to have you here, and we do have jurisdiction over a bunch of things, like Coast Guard, TSA, and then there are a bunch of sub-other entities. And, in all, I think we have 49 percent of your full-time employees come under our, quote, "jurisdiction," or "oversight," whatever you—not "jurisdiction," but "oversight," and 35 percent of your discretionary spending. So, it's a chunk, and I think it makes it—it's important that you're here, because they're extremely important subjects to discuss.

Secretary NAPOLITANO. Yes, sir.

The CHAIRMAN. I welcome you, and I thank you again for joining us today.

And since the creation of the Department of Homeland Security, 8 years ago, we have, in Congress, passed a lot of important pieces of legislation, to try to make our Nation more safe, more secure. As the former Chairman of the Senate Intelligence Committee, which really helps, actually, in this job, and now, as Chairman of this Committee, I sit at an intersection between economic and national security, in a very, very interesting way, and I have a deep appreciation of the many challenges that we face, that you face, and opportunities either lurking or simply on the horizon.

I'm proud to say that the Commerce Committee and its members were deeply instrumental in developing all or part of every major piece of legislation that the Department Homeland Security is responsible for implementing, and we're very acutely aware of that.

During that time, our Nation has made a lot of progress in transportation security, but obviously we have a lot of work that remains.

A complex goal—global transportation network and supply chain—creates enormous security challenges for our Nation. For whatever reason, we seem to be slow to understand that, as a people. And as a government, I don't think we've done our due diligence in terms of supporting DHS, and giving you the money that you need. The Coast Guard's an incredible example of that, and then all of the harbor problems and everything that you—you're struggling to—and doing well, but you've got money problems everywhere.

We have porous borders, both land and sea; they create a lot of inherent risk. Over the last year, I've had the opportunity to discuss with—the state of maritime and port security with Admiral Allen, Commandant of the Coast Guard. I have an enormous regard for that man; I think he has terrific vision and perspective. And, you know, he's very worried—to, sort of, reinforce my concept on a lot of things, but one of them was just the concept of small vessels. There are so many small vessels out there; What do we do about small vessels? What does he do? What do you do? I'll be introducing legislation early next year on this issue, and I look forward, Madam Secretary, to working with you as we develop that.

I also want to highlight that I remain deeply concerned about the state of aviation security, and especially general aviation security and aircargo security. In particular, we remain far too vulnerable in general aviation. I've always felt that. And it's a battle where nobody ever seems to advance the ball, particularly. But, I mean, whenever I've been out to Dulles Airport, I can never remember passing through any metal detector; I never remember having any check on anything. And that should not be. And it's sort of easy; it has—since we all experience that, we notice it, and other people would be inclined to notice that, too, and they may not—they may have ill intent.

The—I think your predecessors shared that view—or, your predecessor—shared that view, and I look forward to hearing your views on this specific problem of the state of aviation security. Both Congress and the Administration must balance important but competing needs, maintaining an efficient flow of commerce while ensuring that no terrorists can enter our country by land, air, or sea. And they can. And we all know that. I understand this balance, and I'm committed that we in Congress do all we can to make sure that it's achieved, and work with you to help you to make sure that it's all achieved.

I understand the GAO, the Government Accountability Office, is releasing a report for the Committee today about the 100-percent-scanning mandate for maritime cargo. That's something that the House is really up on. I have my questions about whether that's doable, and I want to talk about that with you, because it's very—a very important subject, and you can increase your security, if we had all the machinery for it and could afford it, but you might slow down commerce, which I suppose could happen. But, when you're talking about all the ports around the world, it becomes pretty complex.

The GAO highlights the enormous difficulty of meeting this mandate due to the global nature of supply chain logistics and simply a lack of technology, sufficient technology. That does not mean that we should not continue to strengthen our security protocols to prevent high-risk cargo from entering this country, whether by land, sea, or air. That's a big problem. We need to work harder to find ways to balance our security needs with our need to move goods and people efficiently. That's always the challenge. And they are not mutually exclusive. They don't have to be mutually exclusive.

I—you know, I—the two DNIs, President Bush's and President Obama's, both, in an Intelligence hearing in the last Administration and this hearing that are sort of global threats, both of them flat out came and said that cybersecurity is the greatest threat to national security. They—everything else was after that. We hear that. It goes right through our head. We don't do that much about it. And—that various agencies do, and there are, you know, 50 Federal agencies claiming jurisdiction, and 20 Congressional committees claiming—or subcommittees—claiming jurisdiction. So, it's a mess, but it's a mess which stands as our major national security threat.

To date, Congress has not spent as much time on cybersecurity as transportation security. And that has to change. That's our fault. I'm committed to making cybersecurity a focus for this committee and for this Congress; want to work with you on that. The interconnectedness between government and private industry on this critical issue cannot be ignored in the 21st Century. And again, it's the number-one threat. Two different people, 2 years apart, said exactly the same thing—two different Administrations, two points of view.

Along with Senator Snowe, I've been working on legislation that aims to address the threats that we face from cyberterrorists who intend to wreak havoc on our infrastructure. Madam Secretary, as you and I have discussed, I've called the White House to develop a national security strategy, coordinate new roles, renew responsibilities across all boundaries. And the Congress and the White House and every government agency has to be a part of that solution. And that's very easy to say and extremely tough to get people to acquire the necessary discipline to focus. We call for somebody who reports to the President. Well, that becomes controversial: Is that a czar? And I, sort of, don't worry about that. If people say it's the number-one national security threat, to me that's about all you need to know.

Anyway, we have enormous respect for you. I respect you very much. Over the last 8 years, your Department has experienced a lot of growing pains. I know you're the right person to move the agency forward. I'm totally confident of that. I look forward to being your partner—I think we all do—in solving top security challenges.

And I turn now to the distinguished Ranking Member, Senator Hutchison, from the State of Texas.

STATEMENT OF HON. KAY BAILEY HUTCHISON,
U.S. SENATOR FROM TEXAS

Senator HUTCHISON. Well, thank you very much, Senator Rockefeller, for calling this meeting.

Welcome, Madam Secretary.

I want to start by saying, securing our transportation network and infrastructure is essential for our national defense as well as our economic prosperity. Texas is home to 29 ports, including the Port of Houston, which is one of the busiest ports in the world. It ranks first in the United States in foreign water-borne tonnage, and is home to one of the world's largest petrochemical complexes, as well as the U.S. Strategic Petroleum Reserve. A terrorist incident at a major U.S. port could cause a devastating loss of life and deliver a huge blow to our economy.

For years, I've worked with my colleagues on both sides of the aisle to strengthen our Nation's port security and our transportation network. And, while we have made great strides since 9/11, the Department of Homeland Security faces ever-evolving threats and still must meet numerous challenges.

I want to address the transportation security officers, the screeners at airports and other places—in some places—and talk about collective bargaining. While Federal law, of course, prohibits screeners from striking, allowing screeners to collectively bargain through a union could have serious consequences on the Transportation Security Administration's fundamental security mission. I hope that you will talk about that issue and how you intend to address it, because I think it is very important for us to know that our screeners will not able to strike and will not have bargaining that causes work slowdowns and shortages and all of the things that are just short of a strike.

Second—and this is something with which you have much familiarity, I know—is the movement of goods across our land borders. This is an integral aspect of our economy, and must be conducted in a secure, and also efficient, manner. Unfortunately, the wait times at many of our border crossings have increased, while the flow of goods has decreased.

During the floor debate on the SAFE Port Act, I secured an amendment that increased the number of U.S. Customs and Border Protection officers by 275. Now, this is an issue on our land ports. It's also an issue on our water ports, where, in some cases, we are having to share a screener or a transportation Border Patrol person with a port and an airport in the same area. And that's not a good situation.

I welcome your views on how we can meet our resource needs along the Nation's land borders, water borders, and airports, because I think these are the key issues that we must address.

I will ask questions. I will not go further in my statement. But, I do also have questions about the screening of cargo at both our airports and our water ports, as well as, of course, the land ports and the technology for that.

So, you have a huge job, and we know that. That agency is young, and it is an amalgamation of many of our security agencies. But, your responsibility is also critical. So, I welcome you and look forward to asking you questions and hearing what you have to say.

[The prepared statement of Senator Hutchison follows:]

PREPARED STATEMENT OF HON. KAY BAILEY HUTCHISON, U.S. SENATOR FROM TEXAS

Thank you, Senator Rockefeller, for holding this hearing on transportation security. Securing our transportation network and infrastructure is vital for our national defense and our economic prosperity.

Texas is home to 29 ports, including the Port of Houston, which is one of the busiest ports in the world. It ranks first in the United States in foreign waterborne tonnage and is home to one of the world's largest petrochemical complexes, as well as the U.S. Strategic Petroleum Reserve.

A terrorist incident at a major U.S. port could cause a devastating loss of life and deliver a huge blow to our economy.

For years, I have worked with my colleagues on both sides of the aisle to strengthen our Nation's port security and transportation network. While we have made great strides since 9/11 in improving transportation security, the Department of Homeland Security faces ever-evolving threats and still must meet numerous challenges.

First, is the issue of allowing transportation security officers (TSOs), or screeners, to collectively bargain for compensation. While Federal law *does prohibit* screeners from striking, allowing the screeners to collectively bargain through a union could have dire consequences on the Transportation Security Administration (TSA)'s fundamental security mission.

Since the inception of TSA, it has been critical that the agency has a nimble and flexible workforce which can react to emerging threats at a moment's notice. How you intend to address this issue, Madame Secretary, will be of great interest to me and many others on this Committee, as well as the traveling public at large.

Second, the movement of goods across our land borders is an integral aspect of our economy and must be conducted in a secure and efficient manner. Unfortunately, the wait times at many of our border crossings have increased while the flow of goods has decreased.

During the floor debate on the SAFE Port Act, I secured an amendment that increased the number of U.S. Customs and Border Protection (CBP) Officers by 275, and I remain committed to ensuring that CBP has the resources available to carry out a mission that is critical to our Nation's economic and national security.

I welcome Secretary Napolitano's views on how the Department and the Administration intend to best meet the resource needs along our Nation's borders. We simply must have a renewed commitment to tackling the pressing issues along our southern border, challenges that I know the Secretary understands very well.

Again, thank you, Mr. Chairman, for holding today's hearing. I look forward to hearing from Secretary Napolitano on these very important issues.

The CHAIRMAN. Madam Secretary—I should say to my colleagues, that—it may be both parties, but, I know, our party—we're having a Healthcare Caucus—I think is our 1,733rd Healthcare Caucus—at 11:30. And so, what I want to do is, with apology to colleagues on both sides, is to head directly to you, so you can make your statement, and then we'll ask you all kinds of questions.

Secretary NAPOLITANO. Great.

Senator LAUTENBERG. Mr. Chairman——

The CHAIRMAN. We'd be—they're all entered as an—automatically into the record, but the timing—this is—Senator Lautenberg, this is not unusual; this is the way we usually do it. When we're not pressed, we don't do it; but we do do it usually.

Please proceed.

STATEMENT OF HON. JANET NAPOLITANO, SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary NAPOLITANO. Well, thank you, Mr. Chairman, Senator Hutchison, Members of the Committee, for the opportunity to testify on the many actions that the Department is taking to secure

our country and, at the same time, helping to strengthen the foundation of our economic prosperity.

In the interest of time, I have submitted a longer written statement, and ask that it be included in the record.

But, I would like to focus my opening remarks today on one particular issue, and that is the security of containerized maritime cargo.

For years, the Department of Homeland Security and other Federal agencies have been working to mitigate the threat, particularly, of a nuclear device being brought into the country. That was the intent behind Congress's mandate that the Department scan 100 percent of maritime cargo headed into the United States by the year 2012.

Now, when the Department looks to mitigate any threat, we look to two guiding principles: first, a multi-layered approach to security, making us more safe than relying on any single layer; and second, risk management as the best way to make sure that our actions are prioritized and that our resources are focused correctly.

Now, for various reasons, it is difficult to measure, in absolute terms, the risk of a threat of a nuclear device being brought into the United States. But, when we look at our vulnerabilities to this threat, it's clear that we are vulnerable across a number of pathways, and one of these pathways is maritime shipping containers. But, there are others. Private airplanes, as you mentioned, Senator, small boats, as you also mentioned, overland smuggling, are just some examples.

So, when we think about securing the borders of the United States, one useful analogy is that of a home. A house has a front door, but it also has a number of other possible entryways—other doors, the windows, even the chimney. Now, here security has definitely improved at the front door; in this case, the maritime cargo pathway. But, other possible entryways also merit our attention.

So, therefore, we have been building a layered approach to maritime cargo security. We collect advance information on cargo entering the United States—who has it, where it's going, who may have had access to it—so that we can focus on higher-risk cargo. We work with partners in the shipping industry to improve their security. Once we ensure that a company has put strong security measures in place, we focus on higher-risk shipments.

DHS personnel right now are located at 58 ports in 44 other countries working with foreign officials to help ensure the security of U.S.-bound cargo. And on top of these measures, there is the 100-percent-scanning requirement being advanced by pilot projects at five foreign ports.

Now, DHS learned a great deal from these pilots, but it has also encountered a number of steep challenges. Some of these issues relate to the limits on current technology. Technology doesn't exist, right now, to effectively and automatically detect suspicious anomalies in cargo. This makes scanning difficult and time-consuming.

Available technologies are also limited in their ability to see accurately through very dense cargo. And density often can be the measure of something being disguised.

Other challenges are logistical. Many ports do not have a single point through which most of the cargo passes, which means that

100-percent scanning would either severely slow trade or require a redesign of the port. And, on that note, the costs of 100-percent scanning are very steep, especially in a down economy. DHS equipment costs, alone, would be about $8 million for every one of the 2,100 shipping lanes at the more than 700 ports that ship to the United States. So, therefore, DHS is compelled to seek the time extensions, authorized by law, with respect to the scanning provision.

But, the scanning provision has served and is serving its purpose, allowing DHS to focus on this important issue and to gain expertise in it. And so, in the view of the Department, while we need to continue the current efforts, we need to address the security of maritime cargo through a wider lens, how to mitigate the threat against all potential pathways, including, metaphorically, the other doors, the windows, and the chimney.

I look forward to working with you and the Congress on an approach to secure all vulnerable pathways that could be used to smuggle a nuclear device into our country.

Let me, if I might, just briefly mention other actions we are taking to help secure some of the other pathways into our country. These include significant strides in ensuring the security of air cargo. These efforts include work by the Coast Guard to collaborate with our partners at other ports, and with the small-boat community, to identify potential dangers and identify a small-boat strategy. Our efforts also include work with the general aviation community to devise rules to help secure the country from a dangerous weapon being smuggled here via private aircraft.

So, as you can see, we are taking action, but much work remains.

So, I look forward to working with this Committee and with this Congress on addressing this and other threats.

I thank you again for the opportunity to testify. I look forward to addressing some of the issues that you have raised in your own statements and to answering, to the best of my ability, the questions that you might have.

Thank you.

[The prepared statement of Secretary Napolitano follows:]

PREPARED STATEMENT OF HON. JANET NAPOLITANO, SECRETARY, UNITED STATES DEPARTMENT OF HOMELAND SECURITY

Chairman Rockefeller, Senator Hutchison, and members of the Committee: Thank you for this opportunity to testify on the efforts of the Department of Homeland Security to improve security for land, sea, and air transportation, and for cargo, while facilitating travel and trade.

Ensuring our security and facilitating economic activity are mutually beneficial, not mutually exclusive. A safe and secure homeland requires that we maintain effective control of our air, land, and sea borders. Secure, well-managed borders must not only protect the United States from threats from abroad—they must also permit the expeditious and safe flow of lawful travel and commerce. We are pursuing both of these objectives through a broad array of programs in areas of special interest to this Committee. Today I would like to highlight some particular actions we are taking to address our security challenges, and how we working to develop multi-level, risk-based strategies that strengthen our security to the greatest extent possible.

Security Challenges in the Global Supply Chain

The Department has focused on securing the United States from the threat of a nuclear device being brought into this country. Because the potential consequences of such an event would be so grave, we need the best possible strategy to prevent it from occurring.

We know that al Qaeda has expressed interest in obtaining the materials necessary to perpetrate this kind of attack. To combat this threat regardless of who the malicious actor might be, the U.S. Government has put in place a series of programs and initiatives. These include: gathering intelligence on the intent and capability of terrorists or other adversaries; controlling and securing nuclear material at its source; interdicting illicit acquisition of nuclear material; detecting and preventing smuggling into the United States; and preparing to respond to attacks. The detection and smuggling portions of these programs are the predicate for Congress' requirement to scan 100 percent of cargo headed to U.S. ports, and are one part of this overall strategic effort, addressing only one possible pathway through which nuclear material or a device might be smuggled.

We believe that as we look at all the pathways in which nuclear material or a nuclear device might be smuggled, our Nation's security programs should be organized around two fundamental guiding principles: First, that a "defense in depth," or layered, approach is more effective than a single point of security; and second, that efficient and effective risk management is the optimum way to prioritize our actions and allocate our resources.

Assessing the risk of a nuclear device being brought into this country presents some difficulties. When considering "risk," we measure threat and the intent, capabilities, resources, and activities of possible threat actors; we look at our vulnerability to the threat; and we look at the consequences if that threat materializes. In the case of a nuclear device, the potential consequences are great, but the likelihood of an attack is difficult to determine. We know that terrorist organizations aspire to attack us in this way, but because there is little evidence our adversaries have made a significant advancement toward that goal, and because the threat environment is constantly changing, we are limited in our ability to assess the likelihood of the threat based on available intelligence.

At the same time, it is clear that we could be vulnerable to this threat across a number of potential pathways. One of these pathways is through commercial shipping containers that arrive at our seaports. But there are others: General aviation, small boats, and over-land smuggling are examples of some of these vulnerabilities. When protecting against the threat of a nuclear device being smuggled into this country, we must keep in mind that we are dealing with complex systems that have many points of vulnerability. The matter is not as simple as guarding against a threat at a single entryway or other focal point.

The Status of Securing Maritime Cargo

DHS and Congress—through both the SAFE Port Act of 2006 and the Implementing Recommendations of the 9/11 Commission Act of 2007 ("9/11 Act")—have made significant progress in securing maritime shipping containers from being used to smuggle a nuclear device into the United States. Congress imposed multiple requirements—including a mandate to scan 100 percent of containerized maritime cargo [1]—because it saw a vulnerability that needed to be addressed. Because of this mandate, the Department has gained critical knowledge and experience in securing this pathway and has made important progress through a number of initiatives, which are all different layers in our security approach.

First, DHS collects advance information on all containerized cargo entering the United States in order to help assess the threat that each shipment could pose. This process provides critical guidance on where we need to dedicate our security resources. In January 2009, the interim final rule in the marine environment for Importer Security Filing—known as "10+2"—went into effect. This provides DHS with greater visibility into a container's movements and the parties that may have had access to it. DHS then puts this information through sophisticated, automated analytic systems that identify the shipments that pose the highest relative threats. Progress on 10+2 has been very positive—industry participation has been very strong, and we have already received more than 2.8 million filings representing more than 90,000 importers. We anticipate moving forward with a final rule either soon. Through the Customs-Trade Partnership Against Terrorism (C–TPAT), DHS works with the trade community to encourage them to adopt tighter security measures throughout their supply chains. Once we can certify that these measures are

[1] There are important differences between scanning and screening of maritime cargo, as defined by the SAFE Port Act. "Scanning" means utilizing non-intrusive imaging equipment, radiation detection equipment, or both, to capture data, including images of a container. "Screening," on the other hand, means a visual or automated review of information about goods, including manifest or entry documentation accompanying a shipment being imported into the United States, to determine the presence of misdeclared, restricted, or prohibited items and assess the level of threat posed by such cargo. I am using these definitions for these terms for the purposes of discussing maritime cargo.

in place, DHS expedites the inspection of goods from these partners. This allows safer cargo to move more quickly and enables DHS to focus on higher-risk shipments. C–TPAT currently has more than 9,300 industry partners.

Under the Container Security Initiative (CSI), DHS works with 44 foreign customs administrations to jointly identify and inspect high-risk cargo containers at 58 ports before they are shipped to the United States. This provides DHS critical "boots on the ground" at these ports. Importantly, these ports represent about 86 percent of all shipping into the United States.

The 100% Scanning Issue

In advancing the goal of 100 percent scanning, the Secure Freight Initiative (SFI) deploys networks of radiation detection and imaging equipment at five overseas pilot ports.[2] This advanced pilot has encountered a number of serious challenges to implementing the 100 percent scanning mandate.

Certain challenges are logistical. Many ports simply do not have one area through which all the cargo passes; there are multiple points of entry, and cargo is "transshipped," meaning it is moved immediately from vessel to vessel within the port. These ports are not configured to put in place detection equipment or to provide space for secondary inspections. At these ports, scanning 100 percent of cargo with current systems is currently unworkable without seriously hindering the flow of shipments or redesigning the ports themselves, which would require huge capital investment.

Other challenges are the limitations that are inherent in available technology. DHS currently uses both passive radiation detection and active x-ray scanning to look for radioactive material in cargo. An important obstacle is the absence of technology which can effectively and automatically detect suspicious anomalies within cargo containers that should trigger additional inspection. Currently, DHS personnel visually inspect screens for possible anomalies, but the scale and the variety of container cargo make this process challenging and time-consuming. In addition, current x-ray systems have limited penetration capability; this can limit their ability to find a device in very dense cargo. While DHS is pursuing technological solutions to these problems, expanding screening with available technology would slow the flow of commerce and drive up costs to consumers without bringing significant security benefits.

Finally, and on that note, the costs of 100 percent scanning pose a great challenge, particularly in a struggling economy. Deploying SFI-type scanning equipment would cost about $8 million per lane for the more than 2,100 shipping lanes at more than 700 ports around the world that ship to the United States. On top of these initial costs, operating costs would be very high. These include only DHS expenses, not the huge costs that would have to be borne by foreign governments or industry. It is also important to keep in mind that about 86 percent of the cargo shipped to the United States is sent from only 58 of those more than 700 ports. Installing equipment and placing personnel at all of these ports—even the tiny ones—would strain government resources without a guarantee of results.

The Path Forward

Thus, in order to implement the 100 percent scanning requirement by the 2012 deadline, DHS would need significant resources for greater manpower and technology, technologies that do not currently exist, and the redesign of many ports. These are all prohibitive challenges that will require the Department to seek the time extensions authorized by law.

At the same time, it is imperative that we approach the threat of a nuclear device being smuggled into the United States by addressing all possible pathways. The 100 percent scanning mandate has enabled DHS to focus on this issue, adopt the important tool of cargo scanning, and determine how we can best act to mitigate the threat of a nuclear device being smuggled into the United States. In the view of the Department, however, we need to address this issue through a wider lens: how to mitigate this threat across *all* potential pathways. I look forward to continuing to work with Congress to address this threat in such a way.

Similarly, DHS has been taking action to address our other vulnerabilities to the smuggling of a nuclear device. As I explain later in this statement, we are making important progress in securing air cargo. The Coast Guard and our partners at ports of entry are working with the maritime community and with owners of small boats in order to identify potential threats. The Transportation Worker Identification Credential (TWIC) program is helping to ensure personnel security at our own

[2] These locations are Southampton, United Kingdom; Qasim, Pakistan; Puerto Cortés, Honduras; Busan, South Korea; and Salalah, Oman.

ports. DHS is continuing to work with the general aviation community to develop rules that address the risk of bringing a nuclear device being brought into the United States by private aircraft.

All of these efforts are a work in progress. Thus, it is essential that we look at security in a comprehensive manner and allocate our resources according to a strategy that makes the most sense. We cannot define "security" as being able to flip a switch between two options, safe and not safe. Instead, we must evaluate all points of risk and vulnerability, comprehensively across a complex system. Everyone understands the importance of getting it right when it comes to our approach to cargo security. It has long-term and lasting implications for our domestic security, our economy, and our trade relations. I look forward to working with Congress to develop and implement a solution that allocates our resources in a manner that better protects the homeland.

Actions and Challenges in Aviation and Surface Transportation Security

The Transportation Security Administration (TSA) has made great strides this year in addressing key issues in transportation security, a sector critical both to our country's safety and economic prosperity. In the face of an ever-changing threat environment, TSA is dedicated to adopting new procedures and technologies that will protect the public while respecting individual privacy rights and facilitating travel and commerce. Today I will highlight a few important areas in which TSA has been particularly active.

Before I do that, however, I want to express my appreciation to the Committee for supporting the nomination of President Obama's choice to head TSA, Erroll Southers. When he is confirmed, Erroll will bring outstanding leadership to TSA as the agency continues its critical work.

Development of a Dedicated, Effective TSA Workforce

The effectiveness of TSA's security efforts depends first and foremost upon its people. The TSA workforce is the agency's most valuable asset in preventing, detecting, and deterring threats to our transportation sector. Building the TSA workforce is a major priority, and TSA has initiated innovative programs to attract and retain a motivated and a well-trained work force, including a career progression program for Transportation Security Officers (TSOs) and creative pay incentives for part-time TSOs, such as a split shift differential, Sunday premium pay, and full-time health benefits.

TSA has also created programs to address employee concerns. The National Advisory Council (NAC) is a committee of management and TSO representatives from various airports that acts as the liaison for the workforce in presenting to senior leadership new ideas as well concerns relating to existing practices and policies. The Model Workplace program brings staff and leadership together to create a cohesive work environment through local employee councils and training in conflict resolution.

These programs also include an award-winning workers' compensation program that has resulted in significant cost savings, an estimated $19.4 million from FY 2007 to FY 2010. This program includes an innovative nurse case management element that ensures affected employees are receiving proper treatment, medication, and related therapy to facilitate their return to duty after injury, thus reducing time off the job. It also includes a review of all cases on the long term workers compensation roles, which has resulted in the resolution of 67 percent of the cases in existence when the review began in 2007. Immigration and Customs Enforcement (ICE) is working to create a similar program, and we moving to implement this program Department-wide.

Technology Development

The Department is also aggressively moving to improve our technological capabilities in order to address evolving threats to our Nation's security in the air environment. Utilizing the latest technologies allows DHS to more effectively perform its law enforcement and security duties while at the same time facilitating legal travel and trade and expediting security procedures for the traveling public. Aviation security will focus on new technology at airport checkpoints to screen passengers for concealed weapons, explosives, and other prohibited items that might not be detected by a metal detector-providing the capabilities necessary to combat the evolving threats that our intelligence activities have revealed. TSA has gone to great lengths to balance privacy with security in its screening processes, and continues to work on technology enhancements that will offer even greater privacy protections in the future.

Pilot Results for a Biometric Exit Program

At the recommendation of the 9/11 Commission and the requirement of Congress, since the inception of the US-VISIT program, DHS has prioritized the development of an automated capability to record when visitors leave the United States. This is an important tool to addressing visa overstays. By adding biometrics to the current biographic-based system of recording departures, DHS will be able to more accurately and efficiently determine whether foreign citizens have departed the United States.

From May 28 to July 2, 2009, US–VISIT tested biometric air exit procedures at two airports, Detroit Metropolitan Wayne County Airport and Hartsfield Jackson Atlanta International Airport, in accordance with a Congressional requirement that additional biometric collection testing be done prior to publishing a final rule on the topic.[3] In Detroit, Customs and Border Protection (CBP) officers collected passengers' biometrics at the boarding gate. In Atlanta, passengers' biometrics were collected at a TSA checkpoint.

The Department has submitted an evaluation of these pilots to the Senate and House Appropriations Committees and to the Government Accountability Office. The results of the pilot evaluation, combined with the review of a completed public comment period, will inform the final rule that the Department will issue to cover both airports and seaports.

Secure Flight

One of the 9/11 Commission's key recommendations was for the Federal Government to check passengers traveling on commercial airline flights against terrorist watch lists, a responsibility that was previously held by the airlines. In January 2009, Secure Flight became operational, prescreening passenger name, date of birth and gender against government watch lists for domestic and international flights. The program makes travel safer and easier by helping to keep known or suspected terrorists from obtaining a boarding pass and preventing the misidentification of passengers who have names similar to individuals on government watch lists. To date, 18 air carriers have successfully switched to Secure Flight, including one international carrier. Testing is underway with an additional 27 air carriers. Implementation for all covered air carriers is scheduled to be completed by the end of 2010. I would like to thank this Committee for your strong support for the Secure Flight program since its inception and the Government Accountability Office (GAO) for its constructive collaboration during its audit of this important program.

Foreign Repair Stations Rule

TSA is also making progress strengthening aircraft security. On November 18, 2009, TSA published a Notice of Proposed Rule Making in the Federal Register on Aircraft Repair Station security. The proposed rule would establish security requirements for maintenance and repair work conducted on aircraft and aircraft components at domestic and foreign repair stations that are certificated by the Federal Aviation Administration (FAA). It also requires FAA-certificated foreign and domestic repair stations to adopt and carry out a standard TSA security program to safeguard the security of the repair station, the repair work conducted, and all aircraft and aircraft components at the station. The program will require stations to implement strict access controls, provide security awareness training, and allow for DHS inspections.

After 60 days of public comment, we look forward to responding to comments, finalizing the rule and moving forward with the required security audits that to date have been conducted with the voluntary cooperation of many foreign partners.

Large Aircraft Security Program (LASP)

General Aviation (GA) remains a concern to the Department because of its ability to circumvent some of our layers of security and its potential to deliver dangerous people or weapons to the United States. Addressing this concern while maintaining a robust GA sector is one of the purposes of the Large Aircraft Security Program.

TSA has sought out input from GA stakeholders throughout its rulemaking process for LASP, receiving 8,000 comments in response to the initial NPRM, conducting five public meetings and holding additional comment outreach sessions with impacted stakeholders to gain further input and feedback. TSA plans to issue a Sup-

[3] Previously, DHS had proposed a rule in 2008 that commercial air carriers and vessel carriers collect and transmit the biometric information of international visitors to DHS within 24 hours of their departure from the United States. Congress asked DHS to test additional biometric collection before finalizing this rule to ensure that the best available procedures are implemented.

plemental Notice of Proposed Rulemaking before the end of 2010 that incorporates this input and addresses some of the concerns of GA stakeholders.

Air Cargo Screening [4]

Excellent progress continues when it comes to screening air cargo: More than 50 percent of air cargo is now undergoing screening. More than 95 percent of passenger flights fly each day carrying fully screened cargo on board. TSA is moving forward with its Certified Cargo Screening Program (CCSP), but the program will need greater participation from the air cargo industry in order to meet the August 2010 deadline for 100 percent screening of all cargo that is borne on passenger aircraft for flights originating in the United States. To that end, an industry-wide conference will occur in mid-December to encourage participants in the air cargo supply chain to join the CCSP.

Meeting the 100 percent screening requirement for cargo inbound to the United States from foreign countries continues to present challenges. TSA is taking a layered approach to securing this cargo: TSA is increasing security requirements for cargo acceptance, handling, and screening of cargo transported into the U.S. on passenger aircraft. It is strengthening global security standards through collaboration with the International Civil Aviation Organization (ICAO) and through agreements on information sharing and standardization of security with foreign partners. TSA is also working with U.S. Customs and Border Protection (CBP) to examine the feasibility of adapting CBP's automated targeting system (ATS) to provide risk screening on every shipment of cargo.

Improvements in Threat Assessments

The Department is also making progress in preparing a proposed rule to standardize background checks, standards for redress, and fees among all transportation workers who have access to secure areas of the Nation's transportation system in order to reduce redundant background checks and establish consistent standards across the country. This future rule (Universal Security Threat Assessment/Fee Rule) will cover several existing background check programs, such as the Transportation Worker Identification Credential (TWIC) as well as Hazmat drivers, air cargo, airport and airline personnel, and new populations we are required to vet under the 9/11 Act, such as frontline rail and transit workers.

Federal Air Marshal Service

I want to recognize the accomplishments of TSA's Federal Air Marshals Service. In the past 4 years, TSA's highly trained Federal Air Marshals have flown millions of missions worldwide and participated in over 4,000 Visible Intermodal Prevention and Response operations (VIPRs)—45 percent in aviation, and 55 percent in surface transportation.

Surface Transportation

DHS, and in particular TSA, continues to enhance surface transportation security by working with other Federal departments and transportation providers. This will be a major priority of mine during my tenure as Secretary.

Nothing is more important to security across all modes of transportation than well-trained employees. The familiarity of employees with the facilities and operating environments of their specific modes and transportation systems put them in an ideal position to identify and prevent threats. Targeted security training for key employees is one of the most effective measures that we can take to enhance security. To pursue this goal, TSA is drafting an NPRM that will institute employee security training program requirements across all surface modes of transportation: freight railroad carriers; public transportation agencies (including rail mass transit and bus systems); passenger railroad carriers; over-the-road bus operators; and motor carriers transporting highway security-sensitive materials. Training elements for these programs will address security awareness, terrorist behavior recognition, and threat and incident prevention and response.

---

[4] The definition of "screening" contained in the portions of the 9/11 Act that cover air cargo differs from the definition in the SAFE Port Act. In this context, screening means "a physical examination or non-intrusive methods of assessing whether cargo poses a threat to transportation security. Methods of screening include x-ray systems, explosives detection systems, explosives trace detection, explosives detection canine teams certified by the Transportation Security Administration, or a physical search together with manifest verification. . . ." I am using this definition when discussing air cargo.

Actions and Challenges in Maritime Security

In addition to aviation security, maritime security continues to be a major priority for the Department in its overall mission to secure the Nation.

Piracy

The United States is committed to combating piracy, and DHS plays an essential role in this effort. Currently, U.S. Coast Guard personnel augment Central Command's Combined Task Force 151 as part of a U.S. and international force operating in areas prone to piracy.

Because vessel owners and operators have primary responsibility for the security of their vessels and the best defense against piracy is preparedness, DHS has worked with Federal partners to develop guidance for the maritime industry. For example, the Maritime Security (MARSEC) Directive on Vessel Security Measures for High Risk Waters (HRW), which was issued under the authority of the Coast Guard in May 2009 and requires U.S.-flagged vessels to evaluate risk and determine appropriate self protection measures for the vessel when operating in high-risk waters.

This directive requires U.S.-flagged vessels to use security teams (armed or unarmed) in the high risk waters, and we will continue to work with the commercial shipping industry to develop and implement preventative measures to combat piracy. Pirates have proven versatile in adapting their methods so we will continue to provide guidance based on how this threat evolves.

Small Vessel Security

DHS has identified small vessels (those under 300 gross tons) as tools that could be used by terrorists to smuggle either weapons or people, as attack platforms, or as waterborne improvised explosive devices. Last year's attacks in Mumbai and the attack on the U.S.S. *Cole* in 2000 demonstrate how small vessels can be used in terrorist operations. Accordingly, DHS has reenergized the Department Small Vessel Security Strategy, and we are nearing completion on an implementation plan. This implementation plan encompasses programs and actions across Federal agencies, and forms a broad doctrine for reducing this risk.

At the same time, we continue to move forward in other important areas of small vessel security. Many of these programs focus on involving the American boating public in helping to ensure our security from potential attacks that can use small vessels.

For instance, the Coast Guard America's Waterway Watch program provides a way for the recreational boating public to report suspicious and unusual activity when observed on the Nation's waterways. The Coast Guard is also exploring initiatives such as the Citizen's Action Network to improve communications with the boating public.

Our Domestic Nuclear Detection Office (DNDO) has been working on a radiological/nuclear detection pilot program in both the Puget Sound and the San Diego area to strengthen security through existing technology and partnerships with the local maritime community in order to detect vessels which might pose a threat. These steps are greatly expanding detection opportunities and clarifying response roles and options.

The path forward on small vessel security is clear: we will continue to establish and strengthen our partnerships with the small vessel community, engage with our international partners, and develop and implement technologies to reduce the potential threats from small vessels. We anticipate these efforts will lead to enhanced counter-narcotics operations, greater safety for both small and large vessels, and reductions in maritime crimes.

Interagency Operations Centers/SeaHawk

The Interagency Operations Centers (IOC) Project—initiated in response to the requirements of the Security and Accountability for Every (SAFE) Port Act of 2006—has tremendous potential to ensure that our ports are both efficient and secure, and dovetails with one of my major priorities as Secretary: facilitating productive partnerships with state and local government.

DHS plans to deploy the first piece of the IOC project, information integration and management software known as WatchKeeper, Segment 1, to all locations by the second quarter of Fiscal Year 2011. This time-frame that allows for the improvement of the project through more operational testing and refinement.

As scheduled, on October 1, 2009, the Department of Justice pilot "Project SeaHawk" in Charleston, South Carolina was transferred to DHS. The President's FY 2010 Budget provides funding to support the continued operation of IOC Charleston.

SeaHawk provides a collaborative, unified command-based work environment to coordinate vessel and intermodal transportation screening targeting in the Port of Charleston. This successful program has received important support from local jurisdictions as well as from Congress. Using SeaHawk as an example, the construction of an IOC in San Francisco is already underway, and plans are under development to expand the model to New Orleans and Houston-Galveston in the future.

We are also bolstering efforts among DHS components in order to facilitate this interagency model. In March 2009, Customs and Border Protection (CBP) and the Coast Guard entered into a formal agreement to cooperate on the development and deployment of all aspects of the IOC Project and the Secure Border Initiative (SBI). In addition, Coast Guard Sector Los Angeles/Long Beach is being used as a test site to collaborate with DHS Science and Technology to provide mature technology to the IOC Project.

Transportation Worker Identification Credential (TWIC) Program

The successful rollout of the Transportation Worker Identification Credential (TWIC) at Maritime Transportation Security Act (MTSA)-regulated facilities and vessels across the country is a direct result of tremendous coordination and preparation by the maritime community with the Department, the Coast Guard, and TSA.

DHS components are working every day to implement the TWIC program in a number of ways: To date, DHS has conducted checks for and issued over 1.3 million TWICs nationwide. Today, all credentialed merchant mariners and transportation workers who are seeking unescorted access to secure areas of MTSA-regulated vessels and facilities are required to undergo a security threat assessment and receive a TWIC. The Coast Guard is conducting visual TWIC verification checks as part of annual compliance exams and security spot checks and will soon deploy mobile handheld readers to its inspection field personnel.

In addition to reader capabilities being tested by the Coast Guard, a comprehensive TWIC Pilot program is currently underway at various facilities and vessels operations around the country. Laboratory reader tests are largely complete, and 19 readers are approved for use in the pilot. We anticipate a ramp-up of reader installations and installation at all pilot ports January through July 2010, and we are also seeking to augment pilot data by including additional facilities outside those facilities designated as official pilot participants. It is clear that Congress intends for the TWIC Program to use electronic readers to further leverage the security benefits of the program; our goal is to maximize the information learned from the pilot and stakeholder involvement in the rulemaking process.

The excellent cooperation among DHS components on TWIC has yielded significant efficiencies. The Coast Guard and TSA established an exchange process that validates whether workers hold a valid TWIC prior to being issued a Merchant Mariner Credential, yielding an estimated $9 million in cost savings over 5 years, starting in FY 2010.

The U.S. Coast Guard

Over the past year, the men and women of the U.S. Coast Guard have continued their exemplary service ensuring our waterways are secure, both in the interior and along the coasts of the United States and throughout the world. In order to ensure our Coast Guard personnel are able to continue this excellent service, we must procure safe, reliable, and capable equipment and infrastructure for them.

Fleet Modernization

The Coast Guard's readiness is continually threatened by a reliance on assets, systems, and shore infrastructure that are outdated and rapidly becoming less reliable. The cost of operating major cutters is increasing, while the availability of these cutters continues to decline because of an aging fleet that continually needs repairs. This phenomenon has a direct impact on the Coast Guard's ability to execute its mission. Shortages of parts have caused aircraft availability to dip below the Coast Guard's 71 percent target. During the past 12 months, major unexpected repairs for Coast Guard aircraft and cutters have cost the Coast Guard more than $60 million and resulted in a total loss of over three cutter-years of operational time. Long deferred maintenance backlogs also continue to grow. The Coast Guard has gotten the most out of its aging fleet, but is now being forced to make difficult financial and resource-management decisions to buy down risk in the most critical areas.

To overcome these challenges, the Coast Guard must continue efforts to modernize assets and recapitalize its major cutter fleet. In particular, the National Security Cutter, a replacement for the High Endurance Cutter class, is pivotal to ensuring effective enforcement of immigration and narcotics laws. The Response Boats-Medium (RB–M), the replacement for the USCG's disparate collection of mid-size

boats, is already underway and the Maritime Patrol Aircraft (MPA) is already proving its operational value on the Gulf Coast.

Acquisition Reform

Improving acquisition across the Department is a major priority and in the years ahead. These changes will ultimately improve the efficiency and effectiveness of the Coast Guard and the Department.

The Coast Guard, specifically, has consolidated acquisition activities and adopted a blueprint for acquisition reform that make the USCG better equipped to manage costs, schedules, and performance. Additionally, in the past year, Coast Guard established the Aviation Logistics Center, Surface Forces Logistics Center and Asset Project Office, all of which have improved critical support services to operational assets Coast Guard-wide. Moreover, the Coast Guard has endeavored to improve its recruitment, development, and retention of a highly qualified acquisition workforce to ensure we are maximizing the use of taxpayer dollars. Because the Department and Coast Guard have focused on ensuring the appropriate training, skills, and career progression for the USCG acquisition work force, we are seeing positive results. For example, all Coast Guard acquisition projects over $1 billion are now led by DHS Level III-certified program managers (the highest level), a major change from only a few years ago. The Coast Guard's Human Capital Strategic Plan outlines further initiatives through which the USCG will continue to strengthen its acquisition work force.

DHS Efforts to Combat Cybercrime

DHS continues to work extensively with other nations, Federal agencies, state and local law enforcement, the private sector, and our Nation's research and development infrastructure to secure America's cyber networks from a range of threats, including cybercrime. Let me be clear: cybercrime is an evolving and growing threat to our Nation right now, and the Department is working hard to protect the American public, our businesses, and our financial infrastructure from this threat.

Law Enforcement Actions and Partnerships Against Cyber-Crime

Network intrusions can be devastating to both businesses and individuals. Data theft and loss of customer information to any size company can have serious effects to that business. More often than not, those who suffer the most severe consequences are small or medium-sized companies. These companies often lack the resources or expertise necessary to properly protect their networks and data. Our efforts must become more nimble, and law enforcement agencies must be able to adapt to emerging technologies and criminal methods.

Cyber-criminals operate in a world without borders. They can traverse multi-national and multi-jurisdictional boundaries, and the nature of cybercrime cases is becoming more complex. Our response to the growth in cybercrimes and the increasing level of sophistication of this type of threat demands a fully collaborative approach.

The U.S. Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer-related crimes. The Secret Service provides necessary computer-based training to enhance the investigative skills of special agents through the Electronic Crimes Special Agent Program and leads 28 Electronic Crimes Task Forces that collaborate with other law enforcement agencies, private industry, and academia. These approaches exemplify the integrated model that is necessary to combat this threat. The Secret Service works through its Criminal Intelligence Section to identify and locate cyber-criminals and provides state and local law enforcement partners with the necessary computer-based training, tools, and equipment to enhance their investigative skills through the National Computer Forensics Institute. Through international field offices, the USSS maximizes partnerships with international law enforcement, and it uses the US-CERT Liaison Program at Carnegie Mellon University to maximize private-sector support and public outreach.

Outreach to the Private Sector

The mission of securing the Nation's cyber networks requires active dialogue, collaboration, and information sharing between the public and private sectors. Because so much of our Nation's critical infrastructure is in private hands—including our financial infrastructure—it is critical that private entities and the American public know what cybersecurity means for them.

DHS has a number of cybersecurity partnerships underway with the private sector. The Department conducts many of its activities through the Critical Infrastructure Partnership Advisory Council (CIPAC) structure. CIPAC is organized under the National Infrastructure Protection Plan (NIPP) framework to facilitate effective coordination between government infrastructure protection programs and the infrastructure protection activities of the owners and operators of critical infrastructure

and key resources (CIKR). To secure critical infrastructure, the NIPP relies on the sector partnership with the Federal Government. This includes Information Sharing and Analysis Centers, technology and service providers, Sector Coordination Councils, specific working groups, and partners from across the 18 CIKR sectors.

Recent distributed denial-of-service (DDOS) attacks illustrated how government and industry work together to share information. During the attacks, the National Cyber Security Divisions (NCSD), United States Computer Emergency Readiness Team (US–CERT), the National Communications System (NCS), and the National Coordinating Center for Telecommunications (NCC) partnered very well across government and with the private sector to collect information, to understand what was happening, and to share that information with stakeholders—leading to a swift and effective response. The Department is developing a National Cyber Incident Response Plan. This is an interagency effort in cooperation with state, local, and private sector partners to define the cyber incident roles and responsibilities across all sectors. The Department has also launched the National Cybersecurity & Communications Integration Center (NCCIC), a consolidated 24-hour watch and warning center, to improve coordination between Federal and private sector operations centers. The NCCIC brings together interdependent missions of the NCS, NCSD, US–CERT, NCC, Office for Intelligence & Analysis (I&A), National Cybersecurity Center (NCSC) and the private sector to prepare for, respond to and recover from threats to the Nation's IT and communications infrastructure.

Indeed, while DHS works closely with the private sector to share information and to respond to incidents, the private sector also plays another important role. It possesses a great deal of technology and expertise that can help the government in secure its own systems. A vital private-sector partnership can further the development of comprehensive, innovative solutions that improve and expand our Nation's capabilities and keep us ahead of emerging cyber threats. DHS is working with industry to find these solutions. Expanding these partnerships is one of my major priorities as the Department works to secure our Nation's networks from a range of cyber threats.

The Recovery Act and Strengthened DHS Efforts

Finally, I would like to describe to the Committee how the American Recovery and Reinvestment Act has provided critical funds to DHS components that are strengthening our security efforts, facilitating travel and trade and stimulating the American economy.

Congress appropriated $1 billion to TSA to procure and install explosives detection systems and checkpoint explosives detection equipment for checked baggage at airports. TSA will expend around $700 million of these funds to accelerate the modification of existing checked-baggage inspection systems to "in-line" baggage handling systems. TSA will also use around $300 million for its Passenger Screening Program to install upgraded screening technologies at more passenger checkpoints.

Furthermore, the Recovery Act provided $680 million to Customs and Border Protection and the General Services Administration for greatly needed improvements to aging infrastructure, and for the addition of new technology at our Nation's borders.[5] These funds support a wide range of activities related to improving our antiquated port infrastructure: the planning, management, design, alteration, and construction of CBP-owned land ports of entry; procurement and deployment of non-intrusive inspection systems; expedited development and deployment of border security technology on the southwest border; and the procurement and deployment of tactical communications equipment.

Finally, the Recovery Act provided $98 million to the Coast Guard in order to support shore facilities and aids to navigation, as well as to repair, renovate, assess and improve vessels. Of this funding, $88 million will be used for the construction, renovation, and repair of vital Coast Guard shore facilities. The remaining $10 million will help address the needs of the aging High Endurance Cutters.

Conclusion

As you can see, the Department of Homeland Security is moving forward in strong, strategic directions to improve the security of our Nation. Developing smart, strategic ways to secure our country will make our efforts more effective. Improving the security of our transportation sector—air, land, and sea—our supply chains, and our cyber networks will help ensure they continue to be engines for our Nation's economic prosperity.

---

[5] It is important to note that most of the CBP-owned ports of entry are on the northern border, while the General Services Administration controls the facilities of most of the ports on the southwest border. CBP owns 39 northern border ports and four southwest border ports.

Chairman Rockefeller, Senator Hutchison, and members of the Committee: Thank you for this opportunity to testify today. I am happy to take your questions.

The CHAIRMAN. Thank you very much, Madam Secretary.

Let me start out with a relatively small thing, but which is—seems to be very fixable, and we can be a part of that. The drug trade is transporting enormous amounts of cash via vessels on the high seas since our money laundering laws were tightened, post-9/11. I understand, from the Department of Justice—and they had a big conference on this fairly recently, and there was a general agreement that we need to tighten up laws so that we can prosecute. We cannot prosecute, at this point. And so, what I'm asking is that—if you agree that existing laws are insufficient in order to prosecute these criminals, and have you evaluated the threat with the Department of Justice? And do you need additional authority, and can we help with additional authority, so that these criminals can be prosecuted?

Secretary NAPOLITANO. Mr. Chairman, I think that, in that connection, I would defer to the Department of Justice, who would have the actual prosecutorial responsibility.

But, I would inform the Committee that we have seen an uptick in cash going, by sea, that is being used in the drug trade, proceeds of the drug trade; also, drugs coming in by sea. That may be an indicator that many of the measures we're taking at the land border, particularly the Southwest border, are having an impact, because we are now inspecting so much more of the southbound lanes than—way more than ever previously. And we have dog teams, in fact, down at the Southwest border, that are trained to sniff out bulk cash that would be going south into Mexico as the proceeds of the drug trade. So, if there's any good news there, it may be that we're forcing these drug cartels into the ocean.

The CHAIRMAN. All right. Well, then——

Secretary NAPOLITANO. The answer is yes.

The CHAIRMAN. —yes. That's what I wanted. Just one more, and then we'll proceed. Protecting the Nation from security risks posed by nearly 13 million small vessels. I just—I had no idea that there were 13 million small vessels that exist—is, you know, an absolutely monumental task. There are parallel security threats in the general aviation sector, which I have mentioned, which has been long unaddressed as a matter of vulnerability in our aviation industry. So, I want you to respond to that. I understand that you and Admiral Allen are preparing a revised small-vessel security strategy. When will that be finished? That's one question. It's my understanding that DHS has a number of related, but not coordinated, programs to address small-vessel security. How will you integrate these multiple programs into one comprehensive, layered security approach?

Secretary NAPOLITANO. The answer to your question is, the small-vessel strategy—the revised strategy—will be available by the beginning of 2010, so we're well along. We've incorporated comments from the small-vessel community.

We are integrating it into our strategy, in particular, for how we secure the ports. And, Senator Hutchison, you mentioned the ports in Texas and other ports. And again, we get to that theory of the layered-risk approach, measuring risk layering of various things.

But, for example, having different checks and—as vessels enter the ports, particularly some of our larger points—ports, are some of the mechanisms that we're now using.

The CHAIRMAN. All right. And you have the American Waterways Watch. You have the Citizens Action Network, Pleasure Boat Reporting System. Is—and it's all voluntary, of course—is that in any way helpful?

Secretary NAPOLITANO. Those are helpful, yes.

The CHAIRMAN. But insufficient.

Secretary NAPOLITANO. I think we need an overall strategy, and we need to continue to work on the small-boat issue. I would not sit here today and tell you we have solved that problem.

The CHAIRMAN. I thank you.

And—Senator Hutchison.

Senator HUTCHISON. Thank you, Mr. Chairman.

Let's start on the collective bargaining issue. What is your view about the effort to have collective bargaining among the Transportation Security Administration screeners and personnel?

Secretary NAPOLITANO. Thank you, Senator.

I think that we can accomplish collective bargaining, and also do that in such a fashion that we never, at one moment, sacrifice any whit of security, that that can be built into any collective bargaining agreement.

By the way, I'd like to thank the Committee for supporting the nomination of Erroll Southers to be the head of TSA. Obviously, he would have a point position on that particular issue.

Senator HUTCHISON. And what would be the safeguards?

Secretary NAPOLITANO. Well, you can——

Senator HUTCHISON. I mean, I mentioned earlier and addressed that the slowdowns, the sickouts, that sort of thing could have terrible consequences on our security. So, what would you do to protect the traveling public from this kind of diminishment of capability if there were collective bargaining?

Secretary NAPOLITANO. Senator, now—I speak now as a former Governor and a former State attorney general—there are examples, around the country, of collective bargaining agreements with law enforcement agencies that have similar responsibilities, where you have carve-outs, in effect, in the collective bargaining context, to make sure that those types of things are not part of the collective bargaining agreement. We would anticipate, in this context, with the TSOs, that we would be able to reach such an understanding. I will say, by the way, that I worked as a TSO screener last Wednesday, the busiest travel day of the year, and got a little bit of insight into what their life is like on the line. And I also saw a lot of different kinds of shoes.

[Laughter.]

Senator HUTCHISON. Well, let me say, Madam Secretary—I appreciate that—and I think they're doing a great job, because, of course, we all travel so much, and I—I think they are doing a great job.

But, what about the need for flexibility? When there is a threat, a crisis, where you have to do something very quickly, is that on your agenda for protection, as well, if you're going to go into collective bargaining, where someone can be called, they can work more

than the established number of hours? Do you have that kind of flexibility? And are you going to use it?

Secretary NAPOLITANO. Well, the answer is yes, but I would give you an example. Even without a collective bargaining agreement right now, our TSA employees have been very eager to, whenever we've had an emergency and we need to, for example, bring more people down to help staff an airport in a hurricane, when the people who work there have to stay home and work with their families because their house has been destroyed or whatever, and we have never had a problem, in my experience, with employees being willing to move to a place where a crisis is occurring.

Senator HUTCHISON. Well, this is something that we will want to watch very carefully, because I think it has some pretty strong consequences if it's done, and if it's not done right.

Let me ask one more question, and then I will be finished, for this round.

Guantanamo Bay detainees being tried in New York, we all know that the decision has been made to do that. I have two questions.

Number one, were you consulted about the security issues that would surround such a trial, before the Attorney General made that decision?

And second, are you going to take extra measures, during that trial, to protect the traveling public while that is going on in New York?

Secretary NAPOLITANO. Well, the Department of Homeland Security is part of the review team that President Obama established in connection with closing the prison part of Gitmo—not all of Gitmo, but where the detainees are. And the answer is, that we have been working on a host of security issues, and I would anticipate we will be working, not just with DOJ, but also with the City of New York as they prepare for the trials.

Senator HUTCHISON. So, were you consulted in the beginning, before the decision was made to bring them to New York for trial?

Secretary NAPOLITANO. I was not—not in the sense of being consulted as to whether security concerns would preclude the ability to try them in New York, but I'm very comfortable with the decision to try them in New York.

Senator HUTCHISON. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Hutchison.

Senator Lautenberg.

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

Senator LAUTENBERG. Thank you.

Secretary Napolitano, we are very comforted by the fact that you're in charge there. You come with a great record of public service, and you've shown a firm hand since you're here.

So, with that, I ask—2 years ago, Congress acted to require 100-percent scanning of all shipping containers. Now, one of the things that we know is that the—our only threat is nuclear, obviously. The worst attack we've had on American shores was not nuclear, but it was devastating. So, we've got lots of places to look. Threats don't only exist in containers, as you have noted. Can—do we see

any concrete improvements in cargo scanning that had been made since January of this year?

Secretary NAPOLITANO. Well, Senator, I would point to at least two. One is, is that at the end of January of this year, the so-called "10-Plus-2" interim rule went into effect. And I look forward to this January, where we will see even more compliance with that rule. This is a rule that really provides shippers to provide more advance information about what is in a container, who's had access to it, who's packed it, and the like, that we can then use and evaluate against a number of risk measures that CBP now has. And in addition, we have seen our ability now, with—particularly with ARRA money and some other of the monies that the Congress has supplied, an ability to buildup even more on some of our port security. And that has occurred since the beginning of the year.

Senator LAUTENBERG. Let me ask you this. Since the task of securing 100-percent scanning is so monumental, is there a linear approach that says, "Let's look to those ports that come under most concern," they're—I'm sure they're—that we have identified those, would we not? And—but, also, one of the things that I'm—I look at—I'm Chairman of the Transportation—Surface Transportation Subcommittee, and when we look at where we have to be concerned, we've got to look at mass transit, passenger rail, frequent targets of terrorist attacks. Last week, a terrorist bombing of a Russian train resulted in the loss of 26 lives. But, those threats have not influenced our transportation security efforts to the level that, frankly, I think ought to be required, in terms of balance. What steps are being taken now by the Administration to protect those millions of Americans who daily travel by mass transit or passenger rail service?

Secretary NAPOLITANO. Well, Senator, I'd like the opportunity to provide you with a more detailed answer in writing, because a number of steps have been and are being taken from the deployment of grant monies to localities that operate mass transit—buses, you know, those sorts of things, streetcars and light rail and the like. I think, in terms of grants, in 2010 Congress appropriated $300 million for that purpose, and then the Recovery Act added another $150 million in FY–2010 and those grant monies are being deployed.

I think we are also deploying a number of portable monitors, more transit officers, in particularly in large transit hubs; in addition, we have deployed behavioral detection officers under the so-called SPOT program—to give you just an indication of a few of the things that are happening in the land transportation environment where passengers are involved.

[The information referred to follows:]

TSA has established a five-pronged strategic approach to surface transportation:

- Protect High Risk Assets and Systems;
- Elevate the Security Baseline;
- Build Security Force Multipliers;
- Assure Information Flow; and
- Expand Partnerships for Security Enhancement.

TSA is completing a comprehensive risk assessment for the rail sector, as required by Section 1511 of the 9/11 Commission Act, is being incorporated into TSA's Transportation System Security Risk Assessment (TSSRA), which considers a wide

range of terrorist attack scenarios in each transportation mode and evaluates likelihood, vulnerability, and potential consequences. When complete, the TSSRA will provide the context for TSA to compare railroad risks with risks in other modes of transportation. The national strategies, also required by the 9/11 Commission Act, will be incorporated into the corresponding annexes of the upcoming update of the Transportation System Sector Security Plan (TSSSP). The TSSSP, a comprehensive unifying plan, will supersede separate interim strategies and plans for each mode of transportation. These two efforts are consistent with both the 9/11 Act requirement at section 1511 and a recommendation of the Government Accountability Office in its June 2009 report on mass transit and passenger rail security.

TSA comprehensively assesses security in passenger rail through the Baseline Assessment for Security Enhancement (BASE) program, under which Surface Transportation Security Inspectors thoroughly reviews security posture against 17 Security and Emergency Management Action Items that are foundational to an effective security program. More than 120 BASE assessments have been conducted to date. Their results inform development of risk mitigation priorities, security enhancement programs, and resource allocations, notably transit security grants, and enable production and dissemination of a compilation of Smart Security Practices throughout the passenger rail community.

Senator LAUTENBERG. We're out of time, but obviously there's a lot to talk about, and I will take the liberty of inviting you in so that we can have a discussion of some of the issues. And I appreciate your——

Secretary NAPOLITANO. Right.

Senator LAUTENBERG.—good service. Thank you.

Secretary NAPOLITANO. Yes. I look forward to that. Thank you, Senator.

The CHAIRMAN. Thank you, Senator Lautenberg.

Senator Isakson.

STATEMENT OF HON. JOHNNY ISAKSON, U.S. SENATOR FROM GEORGIA

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

Madam Secretary, first, two compliments. I want to thank you for the tremendous effort you and the Department and FEMA made in Georgia during the recent floods. I appreciate your flying down to Georgia and seeing firsthand—I have to tell you, the response of TSA has been—I mean, of FEMA's been fantastic, and we're very grateful. Second, we had an issue with approvals from your Department with regard to African landings by Delta Air Lines in a number of new locations which ran into a lot of difficulty, but, since that time, I want to thank you for the effort you've paid on that. I understand that things with regard to Angola and Liberia are moving along nicely.

And there's another request that's coming—that's all the compliments; the next——

Secretary NAPOLITANO. OK.

Senator ISAKSON.—things are the questions.

Secretary NAPOLITANO. OK, now I'm ready.

[Laughter.]

Senator ISAKSON. Delta has announced it wants to fly into Malabo at Equatorial Guinea on the west coast of Africa, which is a gateway location. Equatorial Guinea has already issued an advance approval and is doing everything that's been asked of them, but they need assistance, not in terms of money, but in terms of the Safe Skies for Africa Program from FAA and TSA. And in a recent meeting in Atlanta, a TSA official announced that three Afri-

can countries would get that assistance. I just want to urge you to make sure Equatorial Guinea is one of the three that gets the Safe Skies Africa assistance so that that can, in fact, take place as soon as possible.

Secretary NAPOLITANO. Thank you.

Senator ISAKSON. And second, we talked a little bit, on the plane going to Georgia, about AirTran and a preclearance request they'd made in Aruba. As you know, in a number of places it's important for preclearance by Customs and Border Patrol so that people transferring back into the United States are cleared when they leave so they can land at a regular terminal gate and leave without going through Customs and Border Patrol or at the point they leave. That request was rejected, which I have been told—and I don't know this to be a fact, so it's not an accusation, it's a rumor—but, that's the first time preclearance has been rejected by TSA.

I would like to ask you—Aruba is a tremendous source of travel back and forth, primarily vacation travel. Atlanta's Hartsfield is a huge point they leave from. There are already 20 to 24 flights on each Saturday, which is the big travel day for tourism, and it would require a little extra personnel, on behalf of the Department, to make the preclearance possible. But, you already have 20 to 24 flights leaving during a 5-hour window on Saturday anyway, so I'd really like for that application to be looked at again, and see if there's anything we can do to facilitate that.

Secretary NAPOLITANO. Senator, we'll be happy to review that application again.

Senator ISAKSON. And last, a question. With the US-VISIT program, we require biometrics, primarily in the form of fingerprints, which are validated when someone comes into the United States by air. It's my understanding that it's the third phase of the program that's getting ready to be announced, which will also require, at airports—when leaving the country—a revalidation of the fingerprint to ensure the person leaving is the person, in fact, that is supposed to be leaving, but that that's not going to be required at our seaports or at our border crossings with Canada and Mexico, on the ground. And 80 percent of the people that come to the United States come either by sea or by the Canadian border or the Mexican border, as I am told. Why would we not check at those borders, as well, when they leave, to validate that the person leaving is, in fact, the person we think they are?

Secretary NAPOLITANO. Senator, I'll get back to you, but let me just—my guess is—my educated guess is that, with respect to the Mexico and Canadian travelers, that the volume, in terms of number of passengers and number of lanes, is such that the logistics of employing that for the exiting visitors at those land ports would be prohibitive. And that's really the bulk of what we're talking about. So.

Senator ISAKSON. Well, I appreciate the answer, and I appreciate your following up on both Equatorial Guinea as well as the Aruba AirTran flight.

Thank you very much.

Thank you, Mr.——

Secretary NAPOLITANO. You bet.

The CHAIRMAN. Thank you, Senator Isakson.

Senator Pryor.

STATEMENT OF HON. MARK PRYOR,
U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Thank you, Mr. Chairman.

And, Madam Secretary, thank you for being here today. It's always good to see you and be with you.

Let me ask a few questions, one about trucking; specifically, trucking with Mexico. There has been some news reports recently that have been critical of the Border Patrol's Customs-Trade Partnership Against Terrorism Program. And the gist of these news reports is that some Mexican gun and drug smugglers are actually using this program because it allows the trucks to get through the border quicker and, I guess, with less security. Are you aware of that? Have you—are you aware of those news reports?

Secretary NAPOLITANO. I'm not aware of those news reports. I am familiar with the C–TPATs program, however.

Senator PRYOR. Well, there has been some that basically are saying now that the cartels down in Mexico have figured out that that's a way to get things in and out of Mexico, so I just wanted you to be aware of that and maybe talk to your folks about, you know, how valid that is and if there's anything that Homeland Security needs to do to make sure that we minimize that type of activity.

Secretary NAPOLITANO. Oh, absolutely, because those are the kinds of programs—again, we're always looking, you know, to improve security, but we also have the responsibility to help trade and commerce——

Senator PRYOR. Right.

Secretary NAPOLITANO.—move. And that is a particularly difficult balance to strike at our land ports. So, we will take a look at those news reports, Senator.

Senator PRYOR. Well, I agree—appreciate that. And I know that we have had some, you know, terrible news out of Russia in the last few days. And Senator Lautenberg asked about that. And it may be a little too early to have lessons learned, based on rail security and bombs on trains or on train tracks, but I would be interested to know, as you follow up with Senator Lautenberg, about, you know, what we can do better, and your assessment of how secure our rail system is in this country.

Secretary NAPOLITANO. Indeed.

Senator PRYOR. And another thing is, there has been some, let's see, DHS IG report that has looked at FEMA's use of four primary sourcing mechanisms: one is warehouse goods; two is mission assignments; three, interagency agreements, and four, contracts. And basically the DHS IG has said that FEMA does not have a clear overarching strategy that can guide decisionmaking on which of these sourcing mechanisms should be used to meet a particular need. Are you familiar with that DHS IG assessment?

Secretary NAPOLITANO. Senator, I'm familiar, generally. I have not read the IG report, but I can say with confidence that the current administrator of FEMA is addressing any and all concerns that have been raised by the IG, and he's doing it very rapidly.

Senator PRYOR. Yes, one of the concerns, I think, that's raised is that, in a disaster, we need to make sure that we can deliver the critical commodities needed in that locality. And I think it raises a question about that.

And the other thing I had for you, generally, on that—in that same vein, is—I know one of the things that we've talked about in this committee previously, and in Homeland Security, as well, is trying to make sure that DHS and FEMA are working with local and State leaders, and doing a better job of coordinating with various industry groups, even like the trucking industry or the retailers, or whoever it may be, to try to make sure that we can all interconnect, when we need to, to get what we need done done at a critical moment. Are you comfortable, are you satisfied that we have been making progress there, and there's sufficient cooperation and communication?

Secretary NAPOLITANO. Senator, I think, and believe very strongly, that we have improved cooperation there quite substantially, both from FEMA itself and through the Office of Intergovernmental Programs. And it's everything from regular e-mails, conference calls, and all the rest. And that kind of cooperation, that linkage up with State and locals, is absolutely key, not just on the crisis management kinds of issues that FEMA is concerned with, but also with the national and homeland security issues that we also need to be working closely with State and locals on. So——

Senator PRYOR. Right.

Secretary NAPOLITANO.—the answer is yes. And that continues to be a priority of ours.

Senator PRYOR. And, of course, that ties in with the H1N1 and other, you know, pandemic threats out there, to make sure we have that coordination, that preparation on the front end.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Pryor.

Senator DeMint.

STATEMENT OF HON. JIM DEMINT,
U.S. SENATOR FROM SOUTH CAROLINA

Senator DEMINT. Thank you, Mr. Chairman.

And thank you, Madam Secretary, for your briefing and your service to our country.

I want to focus just a few minutes on TSA workers, and just a few questions related to them that—I guess the group we're most exposed to, as Congressmen and Senators who fly all over the country; we're with them every week. But, do you believe the current labor policies of your agency adequately protects the rights and interests of TSA workers?

Secretary NAPOLITANO. Senator, we work hard with our employee workforce to address their issues and their interests. And so, we work hard with them on a whole host of things.

Senator DEMINT. Well, do you think an outside agency or group is needed at this point to help establish work requirements or staffing—standardize the staffing functions or actually help to prescribe how the workforce is managed?

Secretary NAPOLITANO. By "outside groups," Senator, do you mean a union?

Senator DEMINT. Yes.

Secretary NAPOLITANO. Senator, as I mentioned to Senator Hutchison—and again, I go back to my experience as a Governor, as a State attorney general, my familiarity with——

Senator DEMINT. Right.

Secretary NAPOLITANO.—these issues. The answer is that oftentimes in the process of interaction with the union, there are issues raised that management didn't have prior knowledge of, but, in any event, all the security-type issues can and are addressed. And security, for an agency like TSA, would always come first.

Senator DEMINT. Well, that's good to hear. And I've certainly seen, the collective bargaining work at the local level, when there's a close working relationship, but we're talking around 50,000 people, here, all over the country. What I've seen since we've implemented the Department of Homeland Security—as you know, in the beginning it was very controversial about unionization, collective bargaining. In fact, we had to suspend all that because there was a belief that, with all the collective bargaining agreements, we could not pull all the agencies together and do all the changes that were necessary.

One of the good aspects of TSA has been their flexibility, their ability to change constantly and use a continuous quality improvement model, step by step, making changes. When you see the variety of airports and the different carriers and the different routes all over the country, the need for flexibility at almost every airport is key. That is completely inconsistent with the collective bargaining idea, where you're going to standardize various aspects of work requirements and the functions. I mean, how can unionization and collective bargaining enhance security at our airports?

Secretary NAPOLITANO. Well, Senator, the answer is, collective bargaining and security are not mutually exclusive concepts, and they're done—these types of agreements are negotiated all the time, all over the United States. And, as I said before, security always is our number-one interest at——

Senator DEMINT. Well—but, the——

Secretary NAPOLITANO.—the Department.

Senator DEMINT.—concern is—it's easier for us, as a Congress, to start a new agency than to try to get another one to change—a lot of times, because of collective bargaining agreements. So, it's—there's really no example of—up here, that—of the flexibility that would be needed. The types of changes and flexibility that I see continuously going on with TSA is certainly going to change, to a degree, if there is a third party involved in the decision-making, which there will be. There's no reason for collective bargaining if there's not some standardization or requirement to appeal to that third party when changes are made.

But, my question to you is not whether or not you've seen it work at a State or local level, but the whole point of Homeland Security, and particularly TSA, is the security of the passengers. And if, in the beginning, in our debate—and every previous administrator of TSA has said that collective bargaining is not consistent with the flexibility and the need to change—you are telling us that you're going to collectively bargain, even though there's apparently no reason to protect workers, that there's not any reason to stand-

ardize various work requirements. Why do we need to bring collective bargaining into this process, when we see TSA making the improvements that it needs to, to make our passengers more secure?

Secretary NAPOLITANO. Well, thank you, Senator for noting the improvements of TSA and the employee workforce we have there. But, again, I'd go back to the basic point, that I do not think security and collective bargaining are mutually exclusive, nor do I think that collective bargaining cannot be accomplished by an agency such as TSA, should the workers desire to be organized in such a fashion.

Senator DEMINT. OK. Thank you for answering my question.

Secretary NAPOLITANO. Thank you.

Senator DEMINT. Yield back.

The CHAIRMAN. Thank you, Senator.

And now Senator Warner.

STATEMENT OF HON. MARK WARNER,
U.S. SENATOR FROM VIRGINIA

Senator WARNER. Thank you, Mr. Chairman. And thank you for holding this hearing.

And it's great to see my former colleague, former gubernatorial colleague, Secretary Napolitano, and congratulations. And I'd echo some of my colleagues' earlier comments about the good job you're doing.

I want to continue on another line of questioning with TSA. Circumstances happened in my State and, I believe, a number of other States, where airports, if they are going through renovations—in my particular State, the Richmond Airport went ahead, at the encouragement of TSA, when they were doing a renovation, and did a next-generation series of improvement of inline explosive detection equipment. And TSA said, "Go for it. Do it." They went for it, did it, 3 or 4 years ago. TSA promised them a reimbursement of close to $4 billion—$4 million. They're still hanging out, waiting for this reimbursement. And this is not the only airport that's fallen into this circumstance. And I raised this with Mr. Southers, when he came by before his—when he was going through—and is still going through—the confirmation process. But, I just want to raise it again at the secretarial level, that there are—and that Richmond Airport is not alone in this circumstance, where airports, at the instigation of TSA, are going through, putting in next-generation detection equipment, and then if TSA doesn't honor their commitment to do the reimbursement, airports, on a going forward basis, are not going to take this kind of step that I think is necessary. Richmond went beyond what was required, kind of went to next-generation; they did it in a much more extensive way. And I just would ask your office to look into this circumstance. And the more we can get these dollars out so that airports get these commitments honored, would be very, very helpful. I don't know if you're familiar with this or have heard from other airports who have raised this concern, but——

Secretary NAPOLITANO. No, Senator. No other airports have raised that concern, but I certainly will——

Senator WARNER. If you could——

Secretary NAPOLITANO.—look into it.

Senator WARNER.—look into it. It's—the Richmond circumstance has been now hanging out for a number of years. We found a series of other airports that—this was not a one-off circumstance, but it would be something I'd love to get some feedback on.

Secondarily, I'm—again, on a parochial basis, and—but an airport that many of my colleagues fly in and out of, Dulles, where we went through an entire new passenger screening system, and put in that, but TSA staffing shortages still make it—we put in the new system; staffing shortages are there, so that folks are not being served in a timely manner. I don't know if that's kind of raised to your radar screen, as well, but I'd ask you to look into that circumstance, as well. When an airport goes ahead and upgrades their system, they've got to make sure they've got personnel to go along with that.

Secretary NAPOLITANO. Indeed. I'll be happy to look into that.

Senator WARNER. All right.

One that—a final point I wanted to raise, and this is one that I know you would be—will be sensitive to, as a former Governor—perhaps not completely applicable, in terms of Arizona—but, one of the things, in terms of vessel escorts, you know, the Coast Guard has been successfully partnering for a number of years with State and local law enforcement to do vessel escorts as we've come into ports. I know, in our major port, in Port of Hampton Roads, the port down in Norfolk, literally 60 percent of the vessel escorts have not been provided by the Coast Guard, but have been provided by State and local law enforcement as transports come in. State and local governments are under enormous financial stress. And I'm just hoping that if this kind of ratio is maintained, not only at Norfolk, but at other ports around the country, that next year's financial budgets at most State levels are going to be even worse than the last couple of years, as you, I know, are well aware. My hope would be that there could be some level of financial support still given to the State and local areas that are clearly doing part of what would normally fall within the Coast Guard's responsibility, to make sure that this very successful Federal/local—Federal/State/local partnership, in terms of vessel escorting, is maintained.

Secretary NAPOLITANO. Senator, yes, I'll be happy to flag that, as well. That activity may already be covered under some of our existing grant programs, but I'll flag it as a concern.

Senator WARNER. We've heard concerns from, again, our local folks, that they may be concerned—that they're not sure, if they get cutbacks in their local and State budgets, that they're going to be able to maintain this kind of partnership. And that would be to the detriment of all of us. So, I appreciate your attention.

And again, thanks, to the Chairman, for holding this hearing.

The CHAIRMAN. Thank you, Senator Warner.

And Senator Brownback.

STATEMENT OF HON. SAM BROWNBACK,
U.S. SENATOR FROM KANSAS

Senator BROWNBACK. Thank you, Mr. Chairman.

Secretary, welcome. Good to see you here. Look forward to continue working with you on the NBAF facility. Got through this year, and we'll be focusing on next year and continuing that pro-

gram to build it and to get it up and running. It seems like, to me, the type of hearing that we're doing now lends itself to that much more credence for a program like that, where you're trying to protect domestic industry and do the research that's necessary to be able to protect against bioterrorism, agroterrorism, and some other facilities and things.

I want to direct your attention to general aviation, if I could. It's one of the main legs of the Kansas economy. It's really been decimated lately, with this economy. Hopefully, it's starting to come back a little bit.

The industry is very concerned about how it is, then, you regulate general aviation, and whether or not you're going to do it in such a fashion that it can no longer really provide the service that it needs to. GA flies all over—90 percent of the airports don't receive commercial flights; they only are reached by general aviation. And so, there's a real convenience factor, and there's a need; and yet, if it's over-regulated at a point that they can't provide that service in a small airport somewhere simply because of cost—it's cost prohibitive—it shuts it down and it makes it less viable.

I know you're aware of this. In October 2008, there was a proposed rulemaking by TSA on the creation of a large aircraft security program intended to strengthen GA security. There was a strenuous reaction from general aviation on that. I think——

Secretary NAPOLITANO. That would be an accurate characterization.

Senator BROWNBACK. Good, I'm glad you got the message, because they were deeply concerned about it, at a time when, already, their sales and problems were mounting, and they constantly say to me, "Just don't kill us. OK? I mean, yes, we need to address security—and we will work with you on common-sense things we can do."

They've put forth, already, seven areas of suggested improvements for that rulemaking: identification of appropriate weight threshold is one that's key to them; possibility of a "trusted pilot" card, if you can look at that and review in it; review of passenger watch lists matching procedures; and prohibited items—that's another one. They've got several others, but—the thing they need is to have balance.

Security is the key thing, and we've got to provide the security, but if you do it in such a fashion that they just can't cost comply with it, you're just going to shut down a bunch of airport services, because they just don't have the ability to match the cost of the security with providing the service. There's only so much freight that it can carry. And I really hope you can work with the general aviation industry on this, because it's just—they view it as life and death to them on the industry in the United States, whether or not they're going to be able to continue to serve 90 percent of the markets that don't have commercial aviation.

I don't know if you have any thought or response to that. I would appreciate your thoughts on it.

Secretary NAPOLITANO. Well, yes—and this was an area, actually, the Chairman pointed out in his opening comments—it has been, in a way—when we look at vulnerability, risk threat, general aviation is a concern that an aircraft could be weaponized or used

to bring something into the country. In terms of that, the comments that we have received from GA have been very useful. We have been working very closely with that community. We've also been doing some reexamination of the modeling that was used, for example, on the weight threshold. The concern there, quite frankly, is, What is the weight by which, if an aircraft were to be flown again into a building, weaponized, how much fuel would be necessary to cause a building to implode, as we saw, tragically, on 9/11? So, they've been looking at remodeling on that, and taking into account some of the concerns or information brought forth by the GA community.

Also, how do you regulate who gets to fly these aircraft around the country? Because of the possibility of bringing in material that would be of danger. So, I think that working with the GA community, taking into account their legitimate concerns about the industry and the airports and the transportation needs of the country, but also taking into account the very significant security issues, we're hoping to get to the right place.

Senator BROWNBACK. We need you to work with us, if you can, because it's an industry that's very dependent upon sensible regulations that can work, but still let the industry be able to fly.

Secretary NAPOLITANO. Indeed.

Senator BROWNBACK. Thanks.

Thanks, Chairman.

The Chairman. Thank you, Senator Brownback.

Senator Snowe.

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

Senator SNOWE. Thank you, Mr. Chairman.

And welcome, Secretary Napolitano. In fact, one of my staff people witnessed your work at TSA firsthand, as a screener. They said you did an excellent job.

Secretary NAPOLITANO. Thank you very much.

[Laughter.]

Senator SNOWE. I would like to address the issue of air cargo screening. I know that the deadline for reaching 100 percent of screening of air cargo is scheduled for August of 2010. And I'd like to have your reaction to the report issued last week by the Department's Inspector General concerning air cargo screening, because raises some significant issues, particularly with respect to securing air cargo.

At this point, your Department has said that more than 50 percent of air cargo has been screened. Is that correct? Is that the figure being screened?

Secretary NAPOLITANO. That is correct.

Senator SNOWE. Because it wasn't clear in the Inspector General's report as to whether or not that had reached the 50-percent level. They also talked about the fact that there are insufficient, or lack of, background checks or training with respect to the personnel handling or accessing that cargo. The report also indicated—but didn't give the number of—drivers were handling or transporting air cargo without the required background checks; the

IG also reviewed the drivers' records and identified that 23 percent did not satisfy the required training and testing requirements.

So, have you had a chance to review this report?

Secretary NAPOLITANO. I have not personally read the entire report. I've read the summary of the report. I've met with TSA about the report, as well as other members of my staff. Many of the recommendations, or many of the concerns, raised in it are things that we are working on right now. And I'll be happy to provide you with kind of a progress report as to where we stand, Senator.

[The information referred to follows:]

Department of Homeland Security—Office of Inspector General

Security of Air Cargo During Ground Transportation (Redacted)—November 2009

APPENDIX B—MANAGEMENT COMMENTS TO THE DRAFT REPORT

U.S. DEPARTMENT OF HOMELAND SECURITY,
TRANSPORTATION SECURITY ADMINISTRATION,
Arlington, VA, October 5, 2009

INFORMATION

MEMORANDUM FOR: Richard Skinner
Inspector General
Department of Homeland Security

FROM: Gale D. Rossides Acting Administrator

SUBJECT: Draft Report: "Security of Air Cargo during Ground Transportation," July 2009

Purpose

This memorandum constitutes the Transportation Security Administration's (TSA) formal agency response to the Department of Homeland Security (DHS) Office of Inspector General (OIG) draft report; "Security of Air Cargo during Ground Transportation" dated July 2009.

Background

The Office of the Inspector General conducted this investigation to evaluate the effectiveness of TSA's efforts to secure cargo while it is handled or transported on the ground, prior to being shipped on passenger aircraft. OIG found that TSA's inspection process has focused on quantity rather than outcomes and ensuring corrective actions. Automated tools to assist inspectors in analyzing results and focusing their oversight efforts on high-risk areas in air cargo security were not adequate. OIG makes six recommendations to strengthen the security of air cargo ground transportation.

Discussion

The *Implementing the Recommendations of the 9/11 Commission Act of 2007* requires TSA to establish a system for industry to screen 100 percent of cargo transported on passenger aircraft in the United States to provide a level of security that is commensurate with the level of security for the screening of passenger baggage. The legislation also set an interim milestone of 50 percent screening to be reached by February 2009. By August 2010, cargo not screened in accordance with TSA-approved processes and procedures cannot be uplifted to a passenger aircraft in the United States.

This is an extensive requirement and, TSA understands there is simply not sufficient capacity or space in airports to meet its demands without carrier delays, cargo logjams, and increased transit times. Therefore, TSA has established a multi-dimensional strategy to reconcile the requirements of the mandate, the security needs of passengers, and the needs of a U.S. economy reliant upon the air cargo industry.

In addition to TSA's existing security regime, we have established three programs to assist in meeting the 100 percent screening mandate and have made excellent progress:

- 100 Percent Narrow-Body Screening—100 percent of cargo uplifted on narrow-body passenger aircraft has been screened since October 2008. This program ac-

counts for 96 percent of passenger flights originating in the U.S. and its territories, and covers approximately 25 percent of the cargo uplifted in the US.

- The Certified Cargo Screening Program (CCSP)—A voluntary program designed to enable certain vetted, validated, and certified facilities to screen cargo prior to delivering the cargo to the air carrier. To date, the majority of air cargo screening is done by air carriers through CCSP.
  - TSA has certified 477 cargo screening facilities through the program.
  - An interim final rule to accelerate the deployment of the program was published in the *Federal Register* on September 16, 2009, and will take effect on November 16, 2009. During initial deployment of CCSP, the onsite facility assessment has been performed by a TSA Field Team staff. TSA expects that during full rollout, assessments will be performed by a TSA-approved validation firm.
- Indirect Air Carrier (IAC) Screening Technology Pilot—an initiative established to test screening technology in a live environment.
  - Participants in this program are working directly with TSA to provide information and data on cargo, commodity-types, and a certain cargo screening technology. Information collected from this pilot will impact future TSA decisions on acceptable screening technologies.
  - There are 91 participating locations receiving approximately $40.6 million in technology assistance.
- TSA Explosives Detection Canine Programs—TSA certified explosives detection canine teams are available to screen cargo throughout the network.
  - 465 law enforcement partner canine teams devote a part of their time to screening cargo; 6 additional teams will graduate in Fiscal Year (FY) 2009.
  - 84 TSA proprietary canine teams are fully dedicated to screening cargo. 36 more teams are authorized and planned for deployment in FY 2010, 19 of which have been hired and are currently in training.

TSA agrees that access control is a vital part of air cargo security. In addition to our operational oversight, we will continue to work to address access control vulnerabilities through clear policy requirements for securing air cargo while it is being stored, sorted, screened, and transported. We are in agreement that the concerns that have been identified with the agency's security threat assessment process should be addressed, and we are providing more guidance and tools to standardize training. TSA's Office of Security Operations (OSO) FY 2010 Regulatory Activities Plan (RAP) incorporates a risk-based approach to inspections. In FY 2009, OSO Air Cargo Compliance has continued to perform Quality Control (QC) and review audits of Performance and Results Information System (PARIS) entries submitted by field elements. Last, TSA will provide cargo inspectors with automated tools that will allow them to dedicate more time with regulated entities.

Overall, we believe that the recommendations contained in the report will provide additional benefit to TSA. TSA has already begun to formulate plans to implement the recommendations contained in the report. Our specific response to each recommendation follows.

Recommendation #1: Mitigate access control vulnerabilities by:

a. Requiring more tests for access vulnerabilities and provide corrective actions to the regulated entities;

b. Placing more focus on entities that are not following the access control requirements; and

c. Requiring inspectors to spend more time promoting awareness of access control vulnerabilities and their impact on cargo security.

TSA Concurs: TSA agrees that access control is a vital part of our layered approach to air cargo security.

a. TSA's Office of Security Operations (OSO) intends to incorporate additional access control testing protocols in the FY 2010 Regulatory Activities Plan (RAP). The RAP is the basis for a Transportation Security Inspectors (TSIs) annual work plan. These additional tests will augment the current system in place. OSO will continue to inspect drivers on their training and knowledge of their security functions.

Inspectors verify compliance with TSA's access control requirements during all comprehensive inspections. In addition, TSA performed a special emphasis inspection (SEI) during FY 2009 Q2 specifically concentrated on access control.

The objective of this SEI was to determine, through realistic testing, if foreign air carriers, aircraft operators, and indirect air carriers (IACs) properly control access to cargo as required under transportation security regulations in 49 Code of Federal Regulations (CFR) and appropriate cargo security programs. Aircraft operators, foreign air carriers and IACs must prevent unauthorized access to cargo in accordance with 49 CFR Sections 1544.205*), 1544.228, 1546.205*), 1546.213, 1548.5, and 1548.15. Additionally, specific requirements regarding access control for employees or authorized representatives are outlined in the applicable cargo security programs. The SEI protocol stipulated that all instances of non-compliance receive a formal investigation. Cases could be resolved with either administrative or civil penalty action. Counseling alone could not be used as a means to close any violations discovered. Finally, SEI results are being used to identify trends in vulnerabilities, assist in identifying corrective measures (*e.g.,* policy or operational), and formulate additional access control testing protocols.

b. TSA is working with our partners to identify new access control mechanisms. Through partnership with outside vendors we are exploring new conveyance security technology. For instance, TSA has authorized a pilot at Detroit Metropolitan Wayne County Airport called M-lock. The M-lock is an electronically serialized locking mechanism which TSA is testing as a tamper evident seal. This device is equipped with programmable specific serial numbers which are displayed on an LED screen with GPS tracking capability, thereby providing enhanced conveyance-level security to Certified Cargo Screening Facility (CCSF)-screened cargo.Currently, TSA is conducting Cargo Vulnerability Assessments at all Cat X and Cat I airports. TSA is committed to mitigating these vulnerabilities. Vulnerability assessment results are being used to improve policy and operational procedures. In addition to our operational oversight, TSA has worked to address access control vulnerabilities through clear policy requirements for securing air cargo while it is being stored, sorted, screened, and transported. Entities participating in the Certified Cargo Screening Program (CCSP), for instance, have strict facility and conveyance access control procedures that include physical security measures (*e.g.,* fences, cameras), employee identification media, chain of custody technology applied to the screened cargo, and secured conveyances (*e.g.,* locked, sealed, or vehicles under escort).

c. As of the date of this report, TSIs have conducted over 2,060 outreach efforts directly related to air cargo security. TSIs currently spend a significant portion of time providing outreach to Indirect Air Carriers and CCSFs both prior to their becoming certified and after. Prior to an IAC becoming approved, they must submit to a TSI Outreach visit. During this visit the TSI reviews all requirements of the applicable Code of Federal Regulations and the Standard Security Program itself. This includes ground movement and access control to air cargo. TSIs review the facility and trucks to determine if in their current state, they would adequately be able to meet requirements. If not, the TSI will work with the entity to achieve the appropriate level of ground movement and access control security prior to approval.

In regard to CCSFs, TSA also has a lengthy application process that requires constant interaction and outreach provided by Principal Cargo Security Analysts (PCSAs). These TSA personnel work with an entity to help them achieve the required security level through outreach and education. A CCSF must be "certified" by a PCSA prior to entrance into the program

Recommendation #2: Improve the security threat assessment process by:

a. Requiring regulated entities to maintain copies of documents reviewed for authenticating the identity of an applicant;

b. Revising the application form to include language noting that failure to provide a social security number may delay or prevent completion of the security threat assessment process and;

c. Requiring TSA's Office of Transportation Threat Assessment and Credentialing to vet applicants.

TSA Concurs: TSA agrees that the concerns that have been identified with the agency's security threat assessment process should be addressed and partially concurs with the recommendations on social security number (SSN)

a. TSA concurs. TSA has just published an Interim Final Rule on Air Cargo Screening, 74 FR 47672, 47701 (September 16, 2009) (Air Cargo Screening IFR) that requires that each aircraft operator maintain copies of the applicant's documents used to verify identity and work authorization.

b. Currently, language in the Privacy Act Notice found in 49 CFR § 1540.203(b)(2)(viii) regarding security threat assessments provides that: "Failure to furnish your SSN may result in delays in processing your application, but will not prevent completion of your Security Threat Assessment." However, TSA's recently published Air Cargo Screening IFR contains the language that the IG recommends: "Failure to furnish this information, including your Social Security Number (SSN) will result in delays in processing your application and may prevent completion of your security threat assessment." 74 FR at 47683.

c. TSA recognizes the importance of utilizing the best method possible to capture and evaluate the history of those who will have ready access to our Nation's air cargo transportation system. TSA will evaluate the process to require for air cargo populations, the costs of necessary system/data base changes that would capture biometrics, and the number of new-hire adjudicators to execute the evaluation process. Additionally, we will review the required increase of fees to cover the vetting process.

Recommendation #3: Enhance training and testing requirements by providing more specific guidance to regulated entities regarding the training and testing requirements. Additionally, TSA should revise the Regulatory Activities Plan to allow more time for inspectors to review these requirements.

TSA Concurs: TSA specifies training and testing requirements in the aircraft operator, IAC, and CCSP security programs. The security programs clearly stipulate the minimum training content, frequency of training, training log requirements, testing frequency, and passing scores for tests. In addition, TSA provides the IACs with TSA-approved training materials and tests for their Security Coordinators, direct employees, and authorized representatives. We are currently developing comparable materials for the aircraft operators and CCSFs. In addition, TSA is beginning the process of developing standardized training and testing, which it plans to require for all regulated parties.

TSIs verify compliance with TSA training and testing requirements during inspections. Noncompliant entities are counseled on how to obtain the proper security training and testing. In addition, TSIs routinely conduct outreach to the regulated air cargo community.

TSA will be revising the FY 2010 RAP. TSA concurs that training and testing of air cargo security requirements are important and will continue to ensure proper regulatory oversight as such. TSA cargo inspectors verify compliance with training and testing requirements as part of all comprehensive air carrier, IAC, and CCSF inspections.

Recommendation #4: Revise the Regulatory Activities Plan to allow more time for inspectors to:

a. Incorporate a risk-based approach that emphasizes the use of historical data and analysis.

b. Provide support and education to the regulated entities to ensure that cargo security requirements are understood and implemented.

TSA Concurs: TSA's FY 2010 RAP addresses these concerns.

a. TSA's FY 2010 RAP incorporates a risk-based approach to inform inspections. We have developed a risk score for every entity regulated under a TSA air cargo security program. Our approach provides a risk score per regulated entity per location, which means that Regulatory personnel will be able to access risk scores specific to their airport. Risk scores are updated quarterly. Inspections will be driven based on the entities score: red, yellow, or green indicators. Inspections will also be driven by local and national intelligence as well as responses to significant national events or identification of systematic vulnerabilities; and

b. TSA will continue to work closely with aviation industry stakeholders to provide support and education.

Recommendation #5: Provide better guidance, training and awareness to all users of the Performance and Results Information System, especially the Transportation Security Inspectors for Cargo. Specifically, develop an action plan for the TSA officials responsible for the Performance and Results Information System to educate the inspectors and ensure optimal use of the available data and analysis. The action plan should also describe:

a. The quality and quantity of information that should be collected and reported to promote data consistency among field locations;

b. Types of information and reports available for inspectors to generate from the system as an effective management tool; and

c. The available analysis in Share Point to improve risk-based planning reporting capabilities.

TSA Concurs:

a. In FY 2009, TSA's OSO Air Cargo Compliance has continued to perform Quality Control (QC) review audits of PARIS entries submitted by field elements. Each quarter, OSO Cargo Compliance selects PARIS inspection reports for airports and Cargo TSIs in each area to review for QC. The inspection QC reviews focus on compliance with the National Inspection Manual (NIM) and RAP requirements. The goal is to review at least one report from each Cargo TSI at each airport by the end of the Fiscal Year. Headquarters (HQ) shares this information with Assistant Federal Security Director's for Inspections upon request and allows them to take appropriate actions when necessary to ensure the PARIS entries submitted by their staff are in compliance with the NIM and RAP requirements.

b. In addition, TSA's OSO Compliance Programs provide PARIS training and guidance materials. This training involves tips on how to more efficiently use PARIS and on generating reports on data contained in PARIS. Training is also provided on the conversion of data extracted from PARIS into Excel Spreadsheet "Pivot Tables." This training provides TSIs with the ability to generate more useful reports on inspection, investigation outreach and incident data, and analyze and organize the reports in a fashion tailored to their needs. This is primarily facilitated through three efforts. First, newly hired TSIs receive PARIS training during the "Transportation Security Inspector Basic Training Program," a comprehensive 4-week training regime at TSA's Security Enforcement Training Academy. This training is conducted via presentation and hands on exercises. This training is continued during the new TSIs official on the job training (OJT). Second, experienced TSIs receive a refresher during recurrent training. Recurrent training is held at least once a quarter at various airports throughout the country with the goal of all experienced inspectors attending at least one session a year. Third, the PARIS program office has developed a comprehensive series of user guides and on-line demos.

Furthermore, in the interest of facilitating swift and effective communications between the PARIS User Community and the PARIS Support staff at HQ, TSA OSO, Inspection Enforcement and Analysis Branch established a PARIS application Help Desk Phone Line in the TSA Phone Network. Field personnel can call HQ personnel and speak to a PARIS support staff member. This additional communication channel is intended to offer an additional convenient means for PARIS users to talk to one of the experts who supports the PARIS program. It does not replace the agency's information technology (IT) single point of contact (*i.e.,* SPOC) and the contractor-based support system that TSA uses for its enterprise IT applications. Rather, it is an opportunity for us to bring increased support to the PARIS user community as it relates to the PARIS application itself. The SPOC remains the first contact for any functional anomalies. Field Inspectors can also reach the help desk support through the PARIS Blog.

c. The Office of Compliance publishes periodic reports into Sharepoint, an internal electronic tracking system. This system is available to all inspectors who perform oversight as well as staff who analyze inspection reports.

Recommendation #6: Provide Cargo Inspectors with automated tools that will allow them to dedicate more time with the regulated entities. Specifically, establish an action plan, with performance milestones, to address the issues preventing the agency from using the personal digital assistant devices to provide more efficient inspection activities.

TSA Concurs in Part: TSA believes that the personal digital assistant devices (PDAs) are antiquated technology and are not efficient. We are moving forward with a plan to provide more modern and advanced tools to our regulatory workforce to improve productivity. These include, but are not limited to:

- Blackberries, with camera feature, for all inspectors.
- Document hand scanners. This device allows TSIs to make copies of records. We have secured one per airport.
- Test phones for special emphasis inspections and small package testing. One test phone per airport with assignment of a new number every 6 months.
- Laptops for all cargo inspectors.

- Dedicated cargo vehicles. We improved the ratio of one vehicle for every two inspectors at the airport.
- One GPS unit per cargo vehicle.
- Air cards for communal use among Regulatory personnel.

These tools have already been procured and will be dispersed to the TSIs by the conclusion of FY 2009.

In addition to securing new productivity tools, TSA's OSO has been working to streamline the record keeping requirements associated with documenting inspections. For instance we revised the PARIS prompts for the passenger and all cargo air carrier and IAC inspection types. Specifically we reduced the number of prompts by 40–50 percent while still capturing all the requirements. This reduces the amount of entry time per PARIS inspection record, and allows the Inspector more discretion on the level of detail to input.

Senator SNOWE. Do you think it's possible to reach the 100-percent deadline for air cargo screening, by August of 2010?

Secretary NAPOLITANO. Well, we're at about 98 percent—we're going to be at about 98 percent, so I think that we'll be very close to it, yes.

Senator SNOWE. Even though the Inspector General indicated that there there's a shortage of TSA personnel, in regard to the screening program?

Secretary NAPOLITANO. Senator, again, subject to something that I'm unaware of, sitting here right now, but I believe we will be able to accomplish that.

Senator SNOWE. The Inspector General's report indicated to me—and this has been a concern of ours, obviously, since September 11 and the 9/11 Commission's recommendations on securing air cargo, that we are still not meeting our goals on an issue that has languished over the years. We've been determined to close this loophole, so it really is important. And I understand that there has been considerable progress made toward this. And we appreciate it, but we want to make sure that we stay on target. And so, given these identifiable deficiencies in the Inspector General's report, it does raise some concerns.

And the Inspector General indicated, as well, that the process is focused on quantity rather than outcomes and ensuring corrective actions. As a result, air cargo is vulnerable to the introduction of explosives and other destructive items before it's loaded onto planes, creating risk for the traveling public.

Secretary NAPOLITANO. Senator, yes, that's what the report says. We have made, I think, even before the report was issued, significant progress on many of the things that are identified in there, because, as you know, reports often lag behind when the concerns were actually raised. And so, we will be happy to provide you with a briefing on the status, but we are making great progress there.

Senator SNOWE. OK. No, I appreciate that.

And one further point on this, because I think it's so essential, is that this report indicates that TSA is unable to properly identify and address vulnerabilities which continue to occur year after year without an effective inspection process for ensuring compliance of air cargo, and went on to say that TSA misses opportunities to strengthen aviation security against the introduction of unauthorized explosive, incendiary, and other destructive substances of items into aircraft cargo.

So, that's obviously quite serious.

Secretary NAPOLITANO. No doubt. We have, again, some responses on that, but, again, I think that the key point is, Are we moving to where there is a 100-percent, or close to it, assurance of air cargo screening in the air environment? And the answer is, we are making significant progress there, that's going to continue to be a priority. And again, I look forward to the confirmation of the new TSA administrator. Obviously, having an administrator in place would be very helpful.

Senator SNOWE. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Snowe.

Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman.

And, Secretary Napolitano, thank you for being here, and thank you for your hard work and dedication. I think the President chose well when he put you into this position, and your background and history and experience, I'm sure, has come into use every single day that you've been in this position.

I think I could ask you questions all day. I think that is probably the result of a State that has something like 75 different ports, you know, 15 of them which are probably working ports for the interests that you care about, a border crossing at Blaine that is probably one of the busiest border crossing between U.S. and Canada in the country, and obviously many other related issues to that. So, I'm going to try to get through these, and if you could——

Secretary NAPOLITANO. I'll keep my answers short.

Senator CANTWELL. Thank you.

The first one has to do with, obviously, the Border and Custom agents, which—you know, we were involved here in increasing the funding to the northern border. We were very—we worked very hard, as a delegation and a group of people, to work on that, for many years, and we were glad we got it. You may remember the Ressam case in which a Port Angeles border agent was able to stop Mr. Ressam, who was the Millennium Bomber, who came through. So, that was before we had the resources. And we're very well aware of dangers there. But, we've also had these incidents—and this weekend's paper, I think, said it best, "Illegal Immigrant Gets $48,000 in Lawsuit Against Border Agents." And so, that's what's going on, that we have this—I appreciate that Alan Bersin visited the State. And so, he's had a lot of meetings, and he's had a lot of discussions with our stakeholders, and we really appreciate that. But, we just have a lot of the Border Patrol acting very far away from the border, in plain clothes, catching people by surprise. In this case, the border agents, you know, in a plain car, plain clothes, came up to these two individuals who were at a bus stop. Now, it's probably within that 150 miles from the border, but it definitely is not next to the border. It was in Mount Vernon, Washington. So, a good—you know, a good 45 minutes, probably, at least, from the border. And so, what I'm asking is, What steps are we taking to ensure that the border agents don't engage in racial profiling and

that all the Department of Homeland Security agencies are targeting the most significant threats at the northern borders?

Secretary NAPOLITANO. Well, obviously, racial profiling is repugnant to the law, and we do not racially profile. And that is part of our training, it's part of our supervision, and it's part of the ethos.

Second, a good border policy requires several things. It requires trained personnel on the ground who are properly supervised. It requires technology. And, in some instances, it requires infrastructure. And so, both at the northern and the southern borders, what we are about is having strategies for those borders, that meet—the fact that they're different types of borders, different terrain, and all the rest—but, nonetheless, that combine, in a strategic fashion, those three elements.

Senator CANTWELL. Well, I think we need to continue to have a dialogue in the Northwest of what's going on, because I think when we—I think when we end up seeing lawsuits being settled against border agents, I think we have issues here that we need to address. And we appreciate your cooperation in working on that.

A second issue, if I could, is obviously that that—that U.S./Canadian border is very important for shipping. And we've had my colleagues talk about security and safety of cargo and container traffic. What are we doing to help ensure that all of North America adopts a regime for border security so that we don't have Asian traffic deciding to go to Canada because they can skip the regime that the United States sets up for border security, only to have that cargo travel all the way across the country and maybe enter, you know, someplace else that doesn't have that border security that you were establishing? So, how do we get that North America regime established?

Secretary NAPOLITANO. Well, if you're talking about, Senator, having almost like a perimeter policy around the continent, obviously that's somewhat difficult. But, I meet——

Senator CANTWELL. I'm saying there are billions of dollars of business of cargo container going in—we're probably—you know, 20 percent of all traffic coming from China. Now, if, just up the road in Vancouver, they decide they're not going to need a security regime, and it's cheaper and faster to go through Vancouver, all that traffic is going to go there, and the U.S. is going to lose that transportation business. So, what are we doing to help make sure that those ports adopt the same kind of regimes?

Secretary NAPOLITANO. Well, Senator, I am meeting regularly with my colleague, my counterpart on the Canadian side, as to what is necessary for security at those ports, because there are certain things that are constants with respect to—be it integrated port security, be it air security, be it land border security, there are certain things that need to be done and need to be accomplished. But, there are differences, and there are very real differences, between the two countries, and I think part of that gets beyond my lane and gets into other departments, in terms of negotiations, as well.

Senator CANTWELL. Thank you.

I see my time is expired, Mr. Chairman. Thank you.

The CHAIRMAN. Thank you, Senator Cantwell.

Senator Klobuchar.

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

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

Thank you, Madam Secretary, for being here. I was just thinking of how full your plate is with H1N1 and the many other issues that you've had, the Fort Hood shooting investigation and a lot of other ongoing changes with our security. So, I thank you for your leadership, and also the leadership you showed when we had the floods in the Red River Valley, which, you remember, involved not just North Dakota, but Minnesota.

Secretary NAPOLITANO. Minnesota.

Senator KLOBUCHAR. Very good.

Secretary NAPOLITANO. Right across the river.

Senator KLOBUCHAR. Exactly.

I'm actually going to mostly focus on the secure watch issue and some of the terrorist watch lists, and the misidentifications on those lists. But, I wanted to start with one quick question about the Canadian baggage rescreening. And this is something that affects my State. We have a state-of-the-art airport and the requirement that checked luggage at appropriately cleared Canadian airport facilities be rescreened before the transfer to a U.S.-based connecting flight, it has frequently caused delayed connections for our passengers arriving, since Canada—because their baggage has to be physically transported from the arrival. And I know that TSA has been working with Canadian authorities for well over a year to reach an agreement that could put in place new technologies for Canadian baggage screening that would meet our own United States security standards. And I wondered if you have any sense of when that agreement will be reached.

Secretary NAPOLITANO. I know about the issue, I know about the discussions, and I don't know when they will come to a conclusion. But, Senator, if you're asking me to see if I can prompt them to hurry up, I'll be happy to do so.

Senator KLOBUCHAR. That's a great answer, thank you.

The watch list redress problems—one of my primary concerns—and I get to know the TSA people very well at my airport, and have had very good relations with them, since I have a hip replacement; so I talk to them every time I'm through the airport, and they do a good job—but, my question was about the No-Fly List. And last year, in response to reports that thousands of U.S. travelers experienced misidentifications each year, I introduced legislation to require the Department of Homeland Security to establish a comprehensive cleared list for innocent travels. The implementation of the Secure Flight Program has been underway for nearly a year now, and TSA officials continue to stress that, once the program is fully operational, these misidentifications will be minimized. And you say, in your testimony, that 18 air carriers have successfully switched to Secure Flight, and that testing is underway with an additional 27 air carriers.

For the air carriers that have not fully switched to Secure Flight, how are passengers being screened against the watch lists? How do you think this is going? We are still, obviously, having some problems.

Secretary NAPOLITANO. Well, Senator, if they're not in Secure Flight—and again, that is a successful program, and I think it demonstrates how, as our Department matures, but also as technology gets better, and also as we get a better sense of what actually needs to be done and what's value added to security, some of these things do get dealt with. But, Secure Flight is going to cover the vast majority of passengers by the time of its full implementation.

Right now, we're in that transitional status, and those passengers that are not on a—in a carrier that has moved over are still being measured the old-fashioned way. But, we've also implemented some computer software, for example, that helps us segregate out often misidentified names, misspellings of names, and things of that nature. And we have also worked to speed up the—and make easier—the appeal process so people can get de-watchlisted.

Senator KLOBUCHAR. Right. And—but, one issue that still remains, the Department of Homeland Security inspector general recently reported that passengers who encounter misidentifications and seek to use the Traveler Redress Inquiry Program—named TRIP—to clear these problems, they said, generally do not benefit from their participation in TRIP. Their cases often languish for extended periods of time. The IG made 24 recommendations. And one of the main problems highlighted was that the cleared list of travelers who have gone through the TRIP process is used by airlines only sparingly to rule out false positives on the watch lists. You have to understand, in our State we have a kid that was going to Disneyland who couldn't go. He was, like, 2 years old—because of—his name was on the watch list. So, we've had a lot of concerns. We—I think we have a lot of common names in Minnesota. We have a lot of Johnsons and things like that. So, we continue to be concerned.

So, do you know what's happening with the IG's recommendations on the TRIP program?

Secretary NAPOLITANO. Senator, let me get back to you on that. I know that we constantly are working to make those sorts of things more consumer friendly, more passenger friendly. But, I'll get back to you specifically on that.

[The information referred to follows:]

U.S. DEPARTMENT OF HOMELAND SECURITY,
Washington, DC, January 19, 2009

Memorandum For: Richard L. Skinner,
Inspector General,
Department of Homeland Security,

From: David Heyman
Assistant Secretary for Policy

Subject: 90-Day Response to the Office of Inspector General's Final Report Entitled: *Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) (OIG–09–103)*

This memorandum is in response to your request that the Department of Homeland Security (DHS) Office of Policy (PLCY), in coordination with Transportation Security Administration (TSA) and Customs and Border Protection (CBP), provide your office with an update on the actions taken or planned to implement the recommendations contained in the Office of Inspector General's (OIG) report entitled *"Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) (OIG–09–103)."*

The OIG had 24 recommendations directed to the Screening Coordination Office (SCO) in PLCY, TSA, and CBP.

- OIG has previously closed recommendations #3, 8, and 14.
- DHS requests closure for recommendation #2, 6, 7, 10, and 23.
- DHS and OIG consider recommendations #1, 11, 12, 13, 15, 16, 17, 18, 19, 20, 21, 22, and 24 to be resolved but open until implementation is complete.
- DHS requests that OIG classify Recommendations #4, 5, and 9 as resolved but open until implementation is complete due to the considerable progress that Secure Flight has made toward implementation.

Recommendations

Recommendation #1: Replace TRIP's current case management system with a system that fully meets the program's functional requirements for case management and workflow, document management, interoperability, and reporting. (TSA)

Update: Implementation is currently underway. It is occurring in two phases: design and acquisition/implementation. TSA is fully funding these phases through a combination of Secure Flight resources and appropriations from the Fiscal Year (FY) 2010 budget.

On September 22, 2009, TSA and IBM Global Business Services began work under a contract to perform the requirements analysis and deliver the solution design for the design phase of the new system. TSA held the kick-off on October 28, 2009 with the IBM team and component stakeholders. IBM submitted the Project Plan deliverable on October 30, 2009 and the Vision Statement on December 4, 2009.

Future deliverables for the design phase are: (1) Current process assessment ("As-Is"); (2) New end-to-end processes ("To Be"); (3) "As Is-To Be" gap analysis; (4) "To Be" system requirements and new system design; and (5) Change Management Roadmap. This phase is scheduled for completion by April 16, 2010.

The Phase 2 target completion date is March 31, 2011. Depending on the results of Phase 1, DHS may be able to accelerate the completion date of the overall project to December 31, 2010.

While DHS believes that a successor case management system will create new efficiencies and improvement metrics reporting, the current system remains operational and sufficient to meet mission requirements for serving the public. The current system allows DHS to receive, process, and respond to redress cases in a timely fashion. Its continued operation mitigates mission-related risks from the duration of this schedule, allowing DHS to follow best practices in designing and implementing the successor system.

Due Date: March 31, 2011

Recommendation #2: Define and communicate strategic and operational management roles for TRIP, and participant and program manager responsibilities, roles, and authorities. (SCO)

Update: DHS has implemented this recommendation through the issuance of the "Charter for DHS Appeals and Redress Process" (Redress Charter), DHS has attached a copy to this letter for your reference (see attachment A).

A working group of Subject Matter Experts (SMEs) from the PLCY/SCO. DHS Privacy Office (PRIV), DHS Office of Civil Rights and Civil Liberties, Office of the General Counsel (OGC), TSA, CBP, Citizenship and Immigration Service (USCIS), and Immigration and Customs Enforcement (ICE) met to develop the Redress Charter. The working group also consulted with the Terrorist Screening Center (TSC) and incorporated TSC's feedback into the final product. The SME working group completed the review draft on October 5, 2009, and PLCY/SCO sent the review draft to the DHS TRIP Governance Board, which is comprised of DHS and component leadership. The Governance Board members completed their reviews of the draft charter on October 22, 2009. PLCY/SCO issued the charter as a memo on December 10, 2009.

Due Date: DHS requests that this recommendation be closed.

Recommendation #3: Seek independent funding for TRIP through a line item in the department's budget or that of one of its components. (SCO)

Update: Funding for DHS TRIP was included in the DHS Appropriations Act, 2010 (P.L. 111–83), signed into law on October 28, 2009. PLCY/SCO confirmed with TSA that the funds have been allocated as planned.

Due Date: Closed

Recommendation #4: Revise aviation security directives to specify how air carriers are to use the cleared list, and develop and apply inspection protocols that monitor air carriers' use of the cleared list. (TSA)

Update: TSA has developed and applied inspection protocols that monitor air carriers' use of the Cleared List. TSA has updated its Transportation Security Inspector (TSI) handbook and issued it to the TSIs in the fall of 2009. Relevant excerpts from the TSI Inspection Handbook on the sections dealing with No-Fly list inspections will be provided to 01G. Please note that these excerpts contain Sensitive Security Information (SST) and should not be released or disclosed without prior approval from TSA.

TSA will address the first part of this recommendation through implementation of Secure Flight, which will transfer the watchlist matching function from the air carriers to TSA. Due to the impending cutover to Secure Flight, TSA opted to develop and apply protocols that monitor aircraft operators' use of the Cleared List in lieu of issuing new security directives.

The Secure Flight Final Rule went into effect on December 29, 2008. In May 2009, the Government Accountability Office (GAO) audit of DHS certification conditions confirmed that TSA generally achieved 9 of 10 statutory conditions and conditionally achieved the 10th condition.[1] In November 2009, after the release of the final GAO report, TSA provided GAO with the additional documentation to demonstrate that Secure Flight has generally achieved Condition #10.

Table 1: List of 10 statutory conditions for implementation of Secure Flight assessed by GAO

Statutory Conditions	
Condition 1:	System of Due Process (Redress)
Condition 2:	Extent of False-Positive Errors
Condition 3:	Performance of Stress Testing and Efficacy & Accuracy of Search Tools
Condition 4:	Establishment of an Internal Oversight Board
Condition 5:	Operational Safeguards to Reduce Abuse Opportunities
Condition 6:	Substantial Security Measures to Prevent Hacking
Condition 7:	Effective Oversight of System Use and Operation
Condition 8:	No Specific Privacy Concerns with the System's Technological Architecture
Condition 9:	Accommodation of States with Unique Transportation Needs
Condition 10:	Appropriateness of Life-Cycle Cost Estimates and Program Plans

The Secure Flight program began operational cutover to certain aircraft operators beginning on January 27, 2009. As of October 31, 2009, all airlines were required to request and collect Secure Flight Passenger Data (SFPD) including full name, gender, date of birth, and Redress Control Number (if available). Secure Flight is being phased-in gradually with implementation for all covered aircraft operators scheduled to be completed by the end of 2010. As of December 4, 2009, twenty aircraft operators have successfully cutover to Secure Flight, including one international carrier. Furthermore, eight additional aircraft operators are in parallel operations with Secure Flight (*i.e.,* aircraft operator is sending passenger to Secure Flight, but not applying Secure Flight Boarding Pass Printing Results), and testing is underway with twenty-nine aircraft operators.

TSA has implemented a public awareness campaign that communicates the benefits of the program as well as the changes it will bring for passengers, aircraft operators, and other members of the travel industry.

DHS understands that, at the time of its field research in 2008, there were considerable unknowns surrounding the schedule for implementing Secure Flight. In the intervening year, Secure Flight has made considerable progress and is on schedule to complete implementation with domestic and foreign aircraft operators by the end of calendar year 2010. Given these changed circumstances since the time of DHS OIG's field research, DHS asks that DHS OIG re-categorize this action as resolved but open until implementation is complete.

Due Date: December 31, 2010

Recommendation #5: Provide more of the cleared list to air carriers, at minimum ensuring that they receive all cleared list records that match the current No Fly and Selectee lists using all required matching routines. (TSA)

Update: The full implementation of Secure Flight in 2010 will transfer the watchlist matching function from the air carriers to TSA, eliminating the need to distribute the lists to the carriers. Per the Secure Flight Final Rule, during normal Secure Flight operations,

[1] For generally achieved, TSA has completed all key activities which should reduce the risk of the program experiencing cost, schedule, or performance shortfalls. For conditionally achieved, TSA has completed some key activities and has defined plans for completing remaining activities, that if effectively implemented as planned. should result in a reduced risk of the program experiencing cost, schedule or performance shortfalls.

Secure Flight matches limited passenger information to government terrorist watchlist maintained by the Terrorist Screening Center (TSC).

Given the changed circumstances since the time of DHS OIG's field research (as discussed in Recommendation #4), DHS asks that DHS OIG re-categorize this action as resolved but open until implementation is complete.

Due Date: December 31, 2010

Recommendation #6: Develop and implement a plan for the Office of Transportation Security Redress to address Secure Flight requirements that, at minimum, provide for notifying current redress applicants that their redress control numbers may be useful in future air carrier reservations, and establishes how TSA will incorporate redress control numbers into the cleared list. (TSA)

Update: The DHS TRIP Program Office has sent letters to all aviation-related redress requestors notifying (or reminding) them of their Redress Control Number (RCN) and explaining how the traveler can use the RCN to help avoid misidentifications when traveling by air. TSA approved the letter in September 2009.

TSA mailed this letter to 56,000 individuals, including both persons who received redress through DHS TRIP and who received redress through other means prior to the establishment of DHS TRIP in February 2007. The DHS TRIP Program Office began mailing it out in weekly increments starting in October 2009 and completed the mailings on December 15, 2009.

The RCN is a mandatory field on the Cleared List that is provided to the Secure Flight program. The Cleared List (along with the RCN information) is used within the Secure Flight matching engine. If a passenger is found to be a possible match to the watchlist, the passenger's information, including their RCN (provided at time of flight reservation) will be made available to the Secure Flight Analyst (SFA) so the SFA can clear the passenger accordingly.

Due Date: DHS requests that this recommendation be closed.

Recommendation #7: Use all cleared list records to assist in ruling out all possible passenger data matches to the watch lists identified through Secure Flight, and evaluate options for applying matching thresholds for cleared list matches to account for possible cleared-list passenger data entry errors. (TSA)

Update: As noted above, Secure Flight currently utilizes all Cleared List records to assist in ruling out all possible passenger data matches that were identified through Secure Flight. These Cleared List records were incorporated into Secure Flight on December 15, 2008. Further, Secure Flight works with the Office of Transportation Security Redress (OTSR) and DHS TRIP Program Office in evaluating all other options to clear passengers.

The Secure Flight matching engine already uses 'near match' matching logic when matching against the Cleared List so that possible data entry errors do not prevent the SFA from reviewing near Cleared List matches during the review process.

Due Date: DHS requests that this recommendation be closed.

Recommendation #8: Establish a process to monitor the currency of Primary Lookout Over-Ride record owner status, and institute periodic inspections to determine whether record owner notifications about changes made to an underlying subject record are acted on appropriately. (CBP)

Update: A process is in place to send notifications to the responsible officer for disconnected Primary Lookout Over-Rides (PLOR) that require attention. CBP field offices monitor a daily report on disconnected PLORs, and these daily reports are also actively reviewed by CBP headquarters personnel. In addition, CBP conducts an annual nationwide review of all PLORs. OIG has closed this recommendation.

Due Date: Closed

Recommendation #9: End the practice of singling out passengers with terrorist watch list lookout-related Primary Lookout Over-Rides for selectee security screening when they are identified as possible No Fly list matches during Advance Passenger Information System vetting. (CBP)

Update: Secure Flight will assume all No Fly and Selectee watchlist matching for international flights for all covered aircraft operators, and travelers will be able to provide their Redress Control Number at booking. TSA is scheduled to complete implementation of Secure Flight by the end of calendar year 2010.

Given the changed circumstances since the time of DHS OIG's field research (as discussed in Recommendation #4), DHS asks that DHS OIG re-categorize this action as resolved but open until implementation is complete.

Due Date: December 31, 2010

Recommendation #10: Ensure that final determinations on whether to create a Primary Lookout Over-Ride in response to a redress complaint reside with employees unaffiliated with field offices that made the original screening or admissibility determination. (CBP)

Update: The redress unit reviews, in coordination with CBP PLOR managers, redress cases in which the field office did not implement a PLOR to determine whether it might be appropriate to overturn that field determination. The relevant excerpts from the Executive Communications Unit's desk guide detailing the procedure will be provided to the OIG. Please note that these excerpts contain For Official Use Only (FOUO) information and should not be released or disclosed without prior approval from CBP.

Due Date: DHS requests that this recommendation be closed.

Recommendation #11: Develop and implement a process for the independent review and adjudication of redress cases related to DHS criminal investigations. (SCO)

Update: The Redress Charter includes a provision that Component Redress Offices ensure the "independent review of cases assigned by the Executive Agent" (*i.e.,* DHS TRIP Program Office).

In December 2009, PLCY/SCO launched the Redress Review. Following the model of previous PLCY/SCO reviews for credentialing and vetting programs, the Redress Review is a cataloguing of programs that have or may be candidates for redress throughout DHS, including but not limited to programs tied to DHS TRIP. It will include the development of recommendations for the enhancement and further coordination of redress services.

Relevant to this recommendation, the Redress Review will provide a process to validate that independent review and adjudication of redress occurs and that standard operating procedures (SOP) document the process.

Due Date: April 30, 2010

Recommendation #12: Use TECS Primary Lookout Over-Rides related to terrorist watch list lookouts to help rule out possible No Fly and Selectee list matches identified through the Secure Flight program's automated passenger data vetting process. (TSA)

Update: TSA and CBP are in the process of exploring how to share information about the results of screening encounters as reflected in the Primary Lookout Overrides (PLOR) and Cleared List. Discussions have occurred among program and information technology subject matter experts to identify and rectify barriers to sharing as appropriate.

PLORs and the Cleared List are tools designed to meet the screening environment in which they are used. For this reason, Secure Flight currently uses the DHS TRIP Cleared List to clear individuals with names or identifying information similar to that of individuals on the No Fly or Selectee List in advance of passenger travel. While PLOR and the Cleared List are both used to clear individuals, they serve two distinctly different purposes. The DHS TRIP Cleared List is focused on clearing those individuals associated with threats to aviation rather. CBP, on the other hand, is responsible for conducting a much broader mission at the border; consequently PLOR records will be a result of a much broader screening activities.

The subject matter experts are engaged in identifying a path forward to enhance information sharing. Finding a solution has proven more complex than the initial expectations that DHS expressed in its Management Comments due to asymmetrical elements in each process related to their respective screening objectives. CBP and TSA are exploring the feasibility of developing the operational and technical solutions needed to meet the intent of the recommendation.

Due Date: March 31, 2011

Recommendation #13: Use the TSA's cleared list data to assist in ruling out possible No Fly and Selectee list matches identified in Advance Passenger Information System (APIS) vetting. (CBP)

Update: In the long term, Secure Flight will assume the watchlist matching function of Advance Passenger Information System (APIS), taking advantage of the already established integration of the Cleared List into the Secure Flight process. As stated in the response to Recommendation #12, in the meantime, CBP and TSA subject matter experts are engaged in identifying a path forward to enhance information sharing relating to PLORs and the Cleared List.

To mitigate any potential negative impact on effectiveness, CBP will continue its current practice of communicating directly with TSA Office of Intelligence to confirm the status of No Fly and Selectee list passengers to resolve potential watchlist matches through APIS.

Due Date: December 31, 2010

Recommendation #14: Create a procedure for officers at ports of entry to learn whether Transportation Security Administration Office of Intelligence analysts have ruled out passengers as the target of a watch list lookout. (CBP)

Update: OIG has stated that CBP's procedures fully address this recommendation and has withdrawn the recommendation.

Due Date: Closed

Recommendation #15: Enhance internal controls on the electronic and manual processes for adding records to the cleared list, ensure that all records considered for addition to the cleared list are subject to identity document verification checks before addition, and conduct intelligence analyst reviews of all possible watch list matches before related redress records are added to the cleared list. (TSA)

Update: DHS TRIP is addressing this recommendation in three ways: 1) a case-by-case quality assurance review of the watchlist; 2) incorporating redundant manual quality assurance reviews of a case prior to inclusion on the Cleared List; and 3) hiring a full-time vetting analyst to focus on internal controls as cases are processed.

The DHS TRIP Program Office has completed a manual review of the Cleared List to ensure its quality over two stages. First, in December 2008 prior to submitting the Cleared List for integration into Secure Flight, DHS TRIP personnel reviewed every record on the Cleared List to verify the presence of required identity documents and to reconfirm that none of the records on it were possible matches to the watchlist. Second, between March and June 2009, DHS TRIP personnel conducted a comprehensive review of all redress records to ensure that all records were accurate and that the appropriate DHS component or State Department office had adjudicated the case.

The DHS TRIP Program Office has incorporated a regime of redundant quality assurance checks into its standard practices. DHS TRIP personnel review all Cleared List records are reviewed a minimum of three times prior to final processing. Reviews occur at the initial triage, quality assurance, and archive stages. Additionally, management conducts spot checks of individual records to ensure that the triage process is working properly.

For 2010, DHS requested and received funding for a Transportation Security Specialist (Vetting Analyst) for the DHS TRIP Program Office. This individual will be located in a TSA Operations Center with close proximity to Intelligence Analysts and will have access to secure data sources. This access to all available data will allow the analyst to verify document submissions, view source data for potential watchlist matches, and work with appropriate intelligence and law enforcement personnel before recommending process adjudication. DHS TRIP has developed a Job Analysis Tool (JAT), which is under review for TSA Human Capital Approval prior to competitive recruitment via USA Jobs.

Due Date: March 31, 2010

Recommendation #16: Automatically compare the cleared list against the No Fly and Selectee lists when changes are made to any list, and institute a process whereby intelligence analysts immediately review matching cleared list records for possible removal from the cleared list or refer them to the Terrorist Screening Center. (TSA)

Update: DHS has taken 2 steps in addressing this recommendation. First, TSA is hiring a DHS TRIP Transportation Security Specialist (Vetting Analyst) to be located in a TSA Operations Center. This individual will be located in a TSA Operations Center with close proximity to Intelligence Analysts and will have access to secure data sources, enabling DHS TRIP to access all available data when verifying document submissions. viewing source data for potential watchlist matches, and working with appropriate intelligence and law enforcement personnel before recommending process adjudication.

DHS TRIP has developed a Job Analysis Tool (JAT), which is under review for TSA Human Capital Approval prior to competitive recruitment via USA Jobs.

Second, DHS TRIP is in the process of upgrading its Information Technology capability (currently projected to be complete by 2Q FY2011). One of the upgrades includes the ability to automatically run a daily comparison of the watchlist and the Cleared List that would result in a conflict report for review by the Transportation Security Specialist (Vetting Analyst). The vetting analyst will be able to quickly determine if a change in the status of any Cleared List individual should be changed.

Due Date: Hire vetting analyst by March 31, 2010. IT upgrade by March 31, 2011.

Recommendation #17: Develop and promptly publish the required System of Records Notice and Privacy Impact Assessment for its redress case management system. (CBP)

Update: CBP has drafted a System of Records Notice (SORN) and Privacy Impact Assessment (PIA) for the Complaints Management System (CMS) to cover CBP redress functions and activities that exceed the scope of traveler redress covered by DHS TRIP and its privacy compliance. These activities include officer professionalism complaints, various "wait time" and other service-related complaints, submitted through the CBP Info Center web page. Final clearance of these documents through CBP is pending completion of initial IT system security requirements for the hosting environment for the CBP Info Center web presence.

Due Date June 1, 2010

Recommendation #18: Prepare and revise TRIP-specific standard operating procedures that describe all redress office requirements in intake and triage; coordination and prioritization; review and adjudication; and closeout, response and reporting. (SCO)

Update: PLCY/SCO conducted a data call for all component SOPs relating to DHS TRIP. PLCY/SCO has also obtained a copy of TSC's SOP to serve as a comparable model. PLCY/SCO created a standardized SOP format to improve transparency and assist in comparability among the component SOPs. The tool allows PLCY/SCO to highlight the gaps in SOP documentation and develop a questionnaire to assist the components in documenting their processes and decision-making criteria for redress.

As discussed previously, PLCY/SCO has launched its Redress Review project. Relevant to this recommendation, the Redress Review will provide a process to validate that SOPs fully document redress processes.

Due Date: April 30, 2010

Recommendation #19: Devise and institute quality assurance checks using the 2007 TRIP quality assurance plan as a resource. (SCO)

Update: OTSR instituted a process where all inquiries received are subject to 100 percent quality assurance check prior to final processing (Cleared List, incompletes, or component/TSC referral).

Further, automated and manual Quality Assurance checks will be included in the requirements for the new DHS TRIP case management system. PLCY/SCO has provided the 2007 TRIP Quality Assurance Plan to inform the work of the design team for Phase I. See Recommendation #1 for additional details about the deliverables and schedule for designing and implementing a successor case management system.

Due Date: March 31, 2011

Recommendation #20: Develop and apply TRIP response letter templates that more fully acknowledge the basis for traveler difficulties, note what actions the government took to review the case, and address the underlying cause for the travel difficulty; but do so without compromising law enforcement investigations or revealing redress-seekers' status in the TSDB. (SCO)

Update: PLCY/SCO led a SME group from PLCY/SCO. TSA, CBI:). OGC, DHS CRCL, and DHS PRIV to review the response letter and recommend changes to improve transparency and customer service. The group also consulted with the Department of Justice's (DOJ) Terrorist Screening Center (TSC) in the course of its work. In reviewing the current letters, the working group has as its mandate to make the tone and content more customer-friendly and transparent without compromising law enforcement investigations or revealing redress-seekers' status in the Terrorist Screening Data base (TSDB).

The SME group reached preliminary consensus on a new draft of the core response letter. It also generated scenario-specific variants of this letter to meet the most common types of situations encountered by redress. The SME group engaged with TSC in November 2009 to confer on the letter package and met with representatives from the TSC, FBI, and DOJ to discuss the proposal in detail on December 16, 2009. The meeting generated some additional clarifications which will be integrated into the proposal. The package was sent to DHS leadership for approval on December 19, 2009.

The package is scheduled to begin the formal DHS approval process on January 15, 2010. Department of Justice will also be approving in accordance with the interagency Memorandum of Understanding on Terrorist Watchlist Redress Procedures. The group briefed the TSC on its proposal. TSC agreed that the changes seemed useful and consistent with past direction but indicated that their leadership and legal counsel would need to review the final product before formal concurrence could be reached.

Due Date: February 26, 2010

Recommendation #21: Develop TRIP case disposition reporting categories that reflect the full range of government efforts to resolve redress-seekers' travel difficulties, and report on this information on a regular basis. (SCO)

Update: Developing disposition reporting categories are part of the Phase I design of a successor case management system for DHS TRIP. PLCY/SCO has provided TSA with its observations about lessons learned from current operations and continues to work with TSA on this effort. See Recommendation #1 for additional details about the deliverables and schedule for designing and implementing a successor case management system. This recommendation would be implemented as part of Phase II scheduled to be completed no later than March 31, 2011.

Due Date: March 31, 2011

Recommendation #22: Collect individual TRIP redress case information on the date completed redress petitions are received, and use this information to calculate overall TRIP case processing times. (TSA)

Update: The current case management system is insufficient for implementing this recommendation for the purposes of calculating overall DHS TRIP processing time. It does not have the necessary fields to distinguish between the dates that a case is opened and when the triage review demonstrates that sufficient information and documentation has been provided to begin the redress review process.

The system currently sacrifices that capability in order to ensure that all cases are tracked whether the file has been completed with the applicant's documentation or not. If additional information is necessary, the cases are tracked as "Pending Paperwork" or, if the applicant has not responded to our request after a significant amount of time, "No Paperwork." If and when the necessary information is received, its status is changed to "In Process."

The capability to implement Recommendation #22 will be included in the requirements document scheduled to be completed February 19, 2010 as part of Phase I of the acquisition of an improved Case Management System (See Recommendation #1). It would be implemented as part of Phase II scheduled to be completed no later than March 31, 2011.

The risk related to the due date is mitigated by continuing to use the current system for calculating processing time. While inexact due to inclusion of the time spent by cases in "No Paperwork" and "Pending Paperwork" status, it still provides useful data for managing the process.

Due Date: March 31, 2011

Recommendation #23: Develop timeliness targets for each redress processing stage, and case review and processing activities for each participating agency and DHS component; and report to participating agencies regularly on the achievement of these targets. (SCO)

Update: DHS has issued interdepartmental policy guidance through the DHS TRIP Governance Board to establish timeliness targets for DHS TRIP and related offices, as well as threshold and goal metrics for meeting those targets. The guidance memo was issued on December 10, 2009. The guidance memo is attached for your reference.

Due Date: DHS requests that this recommendation be closed.

Recommendation #24: Collect and report on redress-seeker impressions of the TRIP website, different aspects of the redress experience, and their overall satisfaction with the program, with the aim of using this information to identify areas for improvement. (TSA)

Update: DHS uses the American Customer Satisfaction index to capture statistically reliable data that can be used to improve the effectiveness of DHS.gov, including web-based information about DHS TRIP. The tool prompts individuals who use the DHS website to provide feedback on their experience. It includes several open-ended questions that allow respondents to comment when they are having issues finding information. DHS's current response rate (through November 2009) is 15 percent on exit response, which is high compared to most websites.

In November 2009, this tool indicated that members of the public were unable to find information describing the Redress Control Number. People were searching for this information because the airlines were mentioning it in their communication efforts related to Secure Flight as new optional field for reservations. As a result of this feedback, DHS updated the website to explain the facts about the Redress Control Number and reassure people that most travelers do not have nor need one.

DHS is in the process of launching a customer satisfaction index specific to the DHS TRIP website. PLCY/SCO, in consultation with TSA and the components, drafted two surveys. One is specific to the redress application process and the other asks questions about the overall redress process. The first survey includes four multiple choice questions to gather statistical information on user satisfaction and three open-ended questions to solicit qualitative information that can help identify areas for improvement. The second survey has five multiple choice and one open-ended questions.

Because the surveys are a "collection of information" from more than 10 members of the public, it is subject to the requirements of the Paperwork Reduction Act (PRA). The PRA process includes submitting an analysis to the Office of Management and Budget (OMB) to obtain an OMB Control Number, publishing a notice in the Federal Register with a 60 day comment period, adjudicating the comments, and publishing a 30-day notice in the Federal Register before the surveys can go live. The PRA clearance process began on December 15, 2009 and is expected to be complete no later than May 31, 2010.

A copy of the proposed surveys are attached.

Due Date: June 30, 2010.

If you have any questions regarding this response, please have a member of your staff contact Ted Sobel in DHS/PLCY/SCO at 202–282–9570.

cc: Marcia Hodges, Supervisory Auditor, DHS GIG

Attachments:

A. Charter for DHS Appeals and Redress Process (re: #2) (Source: PLCY/SCO)
B. Redress Control Number letter (re: #6) (Source: TSA)
C. Timeliness Targets Guidance Memo (re: #23) (Source: PLCY/SCO)
D. Website/Redress Experience Survey (re: #24) (Source: PLCY/SCO, TSA, CBP)

Senator KLOBUCHAR. All right, thank you very much, again. And thank you for your leadership.

Secretary NAPOLITANO. You bet.

The CHAIRMAN. Thank you, Senator.

Senator Udall.

STATEMENT OF HON. TOM UDALL,
U.S. SENATOR FROM NEW MEXICO

Senator UDALL. Thank you, Mr. Chairman. And thank you for holding this hearing.

Good to see you here, Secretary Napolitano. We both share the Southwest as home, and I think you're doing an excellent job with a very, very difficult department there to manage.

I'd like, in my time, to hit a couple of areas. One is REAL ID, and then the TSA approach to whole-body imaging.

As you know, more than 30 States, including New Mexico, are unlikely to meet the December 31st deadline to become materially compliant with the REAL ID Act of 2005. While I understand the Administration would prefer to enact PASS ID Act in lieu of granting an additional extension, the uncertainty surrounding what your Department may or may not do if the legislation is not signed into law is creating confusion for people in the State that are not in compliance.

This is—and I'm sure you've heard a lot about this, too—this is causing a great deal of anxiety with constituents, who are seeing news reports they'll need a passport in order to travel on a commercial airline in the U.S. after the 1st of the year. I believe Senator Bingaman and I sent you a letter on this issue, on Monday.

Will you commit, now, to extending the deadline for compliance with REAL ID if Congress has not addressed the issue by December 31?

Secretary NAPOLITANO. Well, Senator, thank you, and yes, here is the problem. Congress passed REAL ID as a footnote in an appropriations bill, that did not have the benefit of hearings, nor consultation with the States, which caused vast revolt among the States, of which Arizona was one. And so, we went and worked with the Governors, on a bipartisan basis, to fix REAL ID, and that gave birth to a piece of legislation known as PASS ID. It has been through committee, it has been marked up, it is ready for floor action. It deals with a lot of the issues that—it solves the Governors' problems with REAL ID.

I would—before I get to the question of extensions—you know, one of the reasons we had REAL ID, and now PASS ID, is because the 9/11 Commission had a recommendation that we improve the security quality of drivers' licenses. And because REAL ID has been rejected by the States, just by granting extension after extension after extension, we're not getting to the pathway to have more secure drivers' licenses. PASS ID helps us meet the 9/11 Commis-

sion recommendations and, at the same time, addresses issues that were legitimately raised by the states.

And so, what I would prefer to urge the Senate to do, and use this hearing as an opportunity to really urge it to do, is to move to floor action and move PASS ID through so we can get it over to the House. I think it could go very quickly over there. And we could solve this issue, as opposed to extension after extension, which not only doesn't deal with the 9/11 Commission recommendation, but it's just another year of uncertainty.

Senator UDALL. Yes. Well, as you are probably aware, the situation that we're in now, we have healthcare on the floor, where if we tried to move to anything else, I think it would make it much more difficult, procedurally. So, I think if—I don't see us getting to PASS ID on the Senate floor between now and the end of the year, so I think it would be very helpful for you to issue a statement—you might use this as an opportunity to do it—to assure people that, after December 31, they will be able to travel with something other than a passport. I don't know if you want to do that, at this point, but—if you decline, that's fine.

Secretary NAPOLITANO. I think I will not accept that——

Senator UDALL. OK.

Secretary NAPOLITANO.—invitation——

Senator UDALL. OK.

Secretary NAPOLITANO.—at this point in time.

Senator UDALL. Thank you. The—I probably don't have enough time to get you to answer the question, but on whole-body imaging, let me just lay it out a little bit here. You're—TSA is greatly expanding its use of whole-body imaging for primary passenger screening at airports. And Albuquerque is one of the airports where it's doing that. And although TSA has voluntarily taken certain measures to protect passenger privacy, I believe several serious questions should be answered before TSA deploys these whole-body imaging machines more widely. And one of the issues, really, is, if you decline the machine, you get a full-body patdown. And, as you can see, that could—you either—one or the other—that could be very intrusive.

So, I—I'm going to submit the questions to you, because my time's up and I know the Chairman may want to get to other Senators here. But, I hope that you'll give us a prompt response on that.

Secretary NAPOLITANO. Right. And, Senator, in the airports I've been at, observing how that technology is used and that technology is much different than as portrayed in the press but, in any event, it hasn't been a patdown, but you go through the standard magnetometer process. We'll be happy to answer the questions that you have.

Senator UDALL. We'll get you all that information.

Thank you very much. Thanks for your service.

The CHAIRMAN. Thank you, Senator Udall.

Madam Secretary, I'm going to ask you a question which you can't answer, but you want to, desperately. But——

[Laughter.]

The CHAIRMAN. But, you can't, because OMB won't let you. OK? I just——

Secretary NAPOLITANO. I'll——

The CHAIRMAN.—thought I'd catch your attention——

Secretary NAPOLITANO. Yes.

The CHAIRMAN.—by saying—OK?

Secretary NAPOLITANO. Yes, you have.

The CHAIRMAN. The—to me, one of the most enormous problems of your extraordinarily important agency—I mean, the President spoke last night, and he kept coming back to what—"The economy I really want to build is my country's economy," and he really had to do that. And I sort of wanted him to say, "And, by the way, in protecting security, we really need to do much more with the Department of Homeland Security, and give it more resources."

I think it's one of the great anomalies—and, frankly, embarrassments to us, in the Congress, and to appropriators—that they have underfunded you. I mean, everybody loves to pick on FEMA or whatever is going on, but often the reason is—or they give you—they say you've got to have 100-percent container scanning, air cargo, maritime cargo, you know, and the—10,000 more rules and regulations have to pour out of your organization, and it's just—it's an awful way—and you are responsible, in so many ways, for our national security. I mean, the intelligence people aren't. You are. They're meant to, you know, provide information; and you have your own intelligence folks. But, you need money. And my question I want to ask you for is, How much money do you need, and what do you need it for, to be able to do what you are required to do and what you want to do? You'll never get another question so wonderful as that.

[Laughter.]

Secretary NAPOLITANO. Thank you, Mr. Chairman.

Let me just address it in the following fashion, which is to say, one of the things that I have set about to do as the Secretary is to identify the major mission areas of the Department, to align our budget requests with those major mission areas, and to create a longer-term vision for the Department through the Quadrennial Homeland Security Review process. Congress asked us to complete that QHSR by December 31. We are on track to do so.

But, I—here's—you know, the major mission areas of the 23 agencies—22 agencies that we're—combine—really involve counterterrorism, securing the air, land, and sea borders, immigration enforcement while we work for immigration reform, and preparation for, and the ability to respond to, disasters of any type—natural disasters. And what we have been about doing is prioritizing, under each of those, and aligning our budget requests accordingly. And I hope——

The CHAIRMAN. I know what you're doing, and I applaud you for it, but it's not helpful. I mean, you're laying out your priorities, and what I would say is that you're then applying totally inadequate resources to your priorities, because you don't have any choice. And you can't say much, because OMB vets your testimony, as they do with any Cabinet Secretary—and way on down, too—and most people don't know that, that you can't speak your mind.

Well, I don't want to get you fired, but I really do want to—Homeland Security to have the money it needs. And, at some point,

maybe we'll have—maybe you can leave a private letter and stick it under my——

[Laughter.]

The CHAIRMAN.—my office door or——

Secretary NAPOLITANO. Over the transom, right.

The CHAIRMAN.—something. But, it counts, to us. It counts, so that we can put pressure on appropriators to be helpful to you. I'll just leave it there.

Secretary NAPOLITANO. Thank you, Mr. Chairman.

The CHAIRMAN. Because you're in an impossible situation.

I wanted to—did not want to leave Senator Brownback's—you know, if you do any regulation of general aviation—the business will go out of—it'll collapse. I just can't let that pass.

I think you mentioned, 90 percent of airports in Kansas, or whatever it was, were small airports, and they're for the use of general aviation, and its convenience. Yes, it certainly is convenient. It's probably convenient to a lot of people who are running drugs and running guns and all kinds of things. And—but, we can't do anything to increase their screening. Again, I've—out at Dulles, the idea of walking through something, which—you know, a machine that that lady, I guess, walked through, crashed the White House party the other night. No, they don't even have them out there. They don't even have them. So, they—there are two—at any given moment, two-thirds of the airplanes in the air are general aviation. They get all of this attention from air traffic control, just as much as any commercial air passenger and—yes, Kansas, you know, makes a lot of general aviation aircraft, but there's also the question of national security of them. You pointed that out, that they could have fuel on them, they could run into buildings. I'm pointing out that they could be running drugs, they could be running guns, and we don't know about it. We're just—and so, we can't touch them; they're untouchable, because if they—you touch them, they call up all the Senators, who—and Congressmen—who ride on their general aviation things, and say, "Don't you dare do anything with it." And that's exactly the way it works. I mean, I tried to put a 25-cent-per-trip tax on them last year to help pay for our air traffic control system. That got 4 inches down the football field. The telephone calls just quashed it immediately. And at some point, this becomes a—just a little bit more than annoying, when they become somehow sacred because they're fragile. They're not fragile; they're doing very well. And whether they're doing well or not is secondary to the national security concerns that you would have, and that I certainly do have, about them. And I just wondered if you would comment on that.

Secretary NAPOLITANO. Well, Senator, as I suggested to Senator Brownback, the security issues involving GA—general aviation—need to be addressed. There was a proposed rule. It had a strong reaction from that community. We have worked with that community. We are in the process of finalizing that rule. But, I agree with you that, when I look at the overall kind of vulnerabilities and threats involving threats to the homeland, particularly with respect to the larger general aviation aircraft, there are security interests that must be protected, and we are moving to do just that.

The CHAIRMAN. How do you do that? They resist that.

Secretary NAPOLITANO. We do it by—through the regulatory process, and we do it——

The CHAIRMAN. Then how come I don't see it?

Secretary NAPOLITANO. Well, because we haven't finished——

The CHAIRMAN. I see no sign of it.

Secretary NAPOLITANO. Well, we haven't finished the rule yet. But, we will be doing it through a variety of mechanisms.

The CHAIRMAN. I advise you to be bold.

My time has run out.

Senator Hutchison.

Senator HUTCHISON. Thank you.

I wanted to go back to the border wait times. This is something that I know you are familiar with, as well, having been the Governor of Arizona. And my question is, How can you address the border wait times? Because there are trucks backed up for miles, taking hours to get through, and it does make a difference in commerce and people being willing to come across. How are you going to address it, keeping security in mind as well as efficiency of commerce, on our land borders?

Secretary NAPOLITANO. Well, a couple of things. And first of all, between Fiscal Year 2008 and Fiscal Year 2009, we actually saw a reduction in wait times, according to the data I have, a 12.3-percent reduction. And the wait times for commercial trucks—and I think that's what you're focused on, Senator—went from, in 2008, 10.6 minutes to 9.3 minutes on the U.S. side of the border.

Where the wait times can add up is on the Mexican side of the border. And so, working with Mexico, they are now establishing their own customs capacity on that side of the border, which I think will do a great deal to resist—because, as you know, when you go through a land port, you're actually going through two borders; you're going through the Mexican side and the U.S. side. So, the U.S. side, the wait times have gone down, and, I think, will continue to go down, with our greater use of technology. The Mexicans——

Senator HUTCHISON. I really am referring to the Mexican side, because that affects so many of our border retailers, and it's—it's commercial, but it's also people who will shop in the——

Secretary NAPOLITANO. In those areas——

Senator HUTCHISON.—yes.

Secretary NAPOLITANO. Indeed. And so, Mexico is now developing its own customs agency, and deploying them to the border, which they really had not had before, as well as we build out our ports on the northern side of the border, we are working with them to build their infrastructure to match our ports so that they're paired up appropriately.

Senator HUTCHISON. So, we do have an ongoing effort to coordinate better the Mexican side with our side so that we can get some of those wait times down for commerce?

Secretary NAPOLITANO. Yes.

Senator HUTCHISON. OK. It's a big deal on our border. It must have been, in Arizona, as well. Because border retailers on our side get a lot of business from that land traffic; and if you have to wait an hour or two, or more sometimes, it's a problem.

Is there something we need to do to increase coordination? Because there has been a complaint, that's ongoing for a long time, of coordination of working hours between DEA, Customs, and Border Patrol, so that sometimes one group is off on a coffee break while the other group is on, but you have to have all of them. Is there an effort in your Department to address that kind of coordination to better utilize our resources?

Secretary NAPOLITANO. Senator, that coordination should already be occurring under the direction of whoever is the manager of the port. If you have a specific instance or a specific port where you are getting reports that that is not happening, I hope you would let me know about it, and we will follow up.

Senator HUTCHISON. OK. I will do that. Thank you very much. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Hutchison.

And Senator Cantwell.

Senator CANTWELL. Thank you, Mr. Chairman. And thank you for allowing me to ask a second round of questions.

And, Secretary Napolitano, again, thank you for your service and all your hard work.

I'd like to submit a question, if I could, to you about semisubmersible vehicles that are being used in the drug trade. And my understanding is they're growing in numbers. I don't know if we've thought about that as it relates to security, since these are one-way vessels and they can be used for drugs; they could be used for other things. But, I'm going to submit that for the record and maybe get an answer from you.

But, I'd like to bring up two specific cases that are—been really receiving national attention, and see if I could get your help on that.

The first is Ernesto Gamboa. He was an individual who served as a confidential informant, and, for the past 14 years, assisted law enforcement in the dismantling of large and dangerous drug operations. He frequently put himself at risk. He worked with the Washington State Patrol, the Federal Bureau of Investigation, the DEA, and INS, and with the Bureau of Immigration and Customs, ICE. So, his cooperation was critical to the success of Federal prosecutors in seizing hundreds of pounds of cocaine and methamphetamine, as well as large seizures of money and weapons.

During all the time that he was cooperating with law enforcement over that time period, he was promised that he would get help with his immigration status; but, instead, in July he was detained by ICE and placed on removal, despite all of the good work that he had been doing previously for these various agencies. And so, I'm expressing concern over this case, because he's kind of in limbo; he can't work, because he doesn't have paperwork, and he can't get—if he is returned to El Salvador, I'm sure he will likely be killed. And so, if we don't help the Gamboas, who have been the informants for us, how are we going to recruit other people to helping us with finding drug traffickers and criminals?

And so, I would, you know, ask for your help in this case, in understanding what we should do with Mr. Gamboa.

Secretary NAPOLITANO. Be happy to look into it. This goes to the intersection between the Department of Justice and the Depart-

ment of Homeland Security, where Department of Justice DEA doesn't have authority to make immigration representations. Sometimes that gets lost in the shuffle. DEA needs to bring ICE in, or vice versa sometimes. So, I think that illustrates, perhaps, what is happening with Mr. Gamboa. I'll be happy to look into the situation.

Senator CANTWELL. Thank you.

The second one is a case, Alonso Chehade, who—you know, we talked about this border issue in my first round of questioning, and Senator Murray and I have asked you to defer the removal of Alonso Chehade until the end of the 111th Congress. He is a case that would be—if the DREAM Act was law, he would obviously have the relief of that legislation. But, he's a 22-year-old Peruvian national who resides—who's resided in the United States since childhood. And earlier this year, he literally took a wrong turn on I–5 and was detained when he accidentally crossed into Canada. And so, now he faces deportation. He graduated from high school with honors, attended Olympic Community College, earned his bachelors degree from the University of Washington. And so, it has generated a lot of media attention in our State. And so, I'm hoping that we can defer action on his case until the 11th—111th Congress—to see if we can get the DREAM Act passed. And so, maybe Mr. Chehade, who has come to the United States as a child, not of his own doing, but has now been through our whole education system, will not, because he took a wrong turn on a freeway—will be able to stay in the United States.

Secretary NAPOLITANO. I think his removal will be, or has been, deferred. I will double check on that, Senator.

Secretary NAPOLITANO. But, the situation you describe illustrates why President Obama is eager to have the Congress take up the whole issue of immigration and immigration reform. These situations happen in my Department every day, day in and day out.

Senator CANTWELL. Well, I appreciate that. And I appreciate you looking into this further. I think he's gotten a temporary deferral, but I think that'll run out in January.

Secretary NAPOLITANO. That may be right. I'll take a look.

Senator CANTWELL. If you could, thank you.

I thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Cantwell.

Senator McCaskill may be on her way. In the meantime, I have one more question to ask.

The—are you OK on time?

Secretary NAPOLITANO. I'm fine.

The CHAIRMAN. OK. The—this is cybersecurity. And this doesn't appear to be a very important question, but it is to me. Again, I go back to George Bush's Director of National Intelligence, Barack Obama's Director of National Intelligence, saying the number-one threat to this country is not al Qaeda, it's not dirty bombs, it is cybersecurity. Huge importance. More or less ignored by the press, a somewhat disinterested public in that, because they can't wrap around those two words. And you have some responsibility for that.

Now, my question is very specific, and you may not want to answer it, but it's—I think we—I don't—I'll tell you how I feel about it. You all had a big conference, and you decided that you'd get

somebody who would report to be responsible for cybersecurity but who would report to the National Security Council and to the National Economic Council, to which I say, "Goodbye focus on cybersecurity." I mean, I've been through that trip before. I've seen what happens. It just—you know, by the time the Pentagon takes their chunk and—you know, it's—it just—it won't work.

Senator Snowe and I, working on—are working on legislation. We'd like to work with you on it. We say that there ought to be somebody who reports only to the President.

Now, there's that part of this world which, "Oh, there's another czar," to which I would say, "Well, if that's another czar, then that's the one you want to have, because that's the number-one national security threat to our country, and will remain so." People have no idea what they can do. They read about it. It hasn't happened in their community, so they forget about it and go on, concentrate on al Qaeda and Taliban, and, you know, all kinds of things, but not on cybersecurity, which is the main threat.

So, I want to say to you that I feel very strongly that there ought to be somebody who reports directly to the President, who has that responsibility, who doesn't try to mix the military and the intelligence and the National Economic Council, because that will—he'll wander off into nothing being done or money not being spent. I think, when you have somebody who reports to the President, it's like the Office of Science and Technology. That's a—he's not a—that's not an—Dr. John Holdren is not an agency, he's a free-floater; he can walk in and out of the Oval Office anytime he wants. But, he's doing science and technology, which you just—affects everything we do in our country, including cybersecurity.

Secretary NAPOLITANO. Indeed.

The CHAIRMAN. And I think that—I think that we ought to have somebody who reports to the President. I want to say that loudly and clearly to you. You don't have to respond, if you don't want, to that view. I think the idea of having it at a lesser stature with a more diverse number of bosses is a very bad idea, and that we won't make progress, because it's the one area of national security where the public really isn't there yet. The press isn't there; they're not interested. It's yesterday's news story. Somebody hacks into something, and then you get 2 or 3 days, and it's gone. And that's a terrible threat—a terrible thing to do to this Nation. So, I just—I want to make that statement. If you'd care to respond to it, I'd be happy. But, that's what our legislation is going to say.

Secretary NAPOLITANO. Well, Mr. Chairman, I would be happy to work with you on that legislation. I think your assessment of cybersecurity as a threat is an accurate one. I would be happy to brief you and your staff on the extensive efforts we have taken within DHS to deal with the civilian side of government and the protection of that, the *.gov* side, as well as our interaction with the private sector. You know, 85 percent of the critical infrastructure in the country is in the hands of the private sector, and they're totally network-dependent. You think of utilities, water companies—and I could go on and on and on. I know you understand what I'm addressing. And so, we have been involved in a series of critical infrastructure meetings over the last 2 months, myself included, with the private sector, with respect to their own network security, and

how we work together to improve that. So, I couldn't agree with you more about the severity and nature of the threat, and I think it is going to be part of our ongoing threat environment.

The CHAIRMAN. I think the private sector will be helpful, but I have to—and this is not really quite fair of me, but—about 10 years ago, I was worried about that and about—generally, about powerplants and chemical plants that had—backed up to the Ohio River. And if you go between—from Pittsburgh, in the Allegheny River, down to Cincinnati, that's about 200 miles—or maybe it's 300 miles, I have no idea, but it's a long way—and there are hundreds and hundreds of powerplants and chemical plants. And three Coast Guard cutters that have, you know, machine guns on the front, heavy machine guns—three—now, they can't go 24 hours a day, so that means there's an average of one every 8 hours—to do—patrol all of the Ohio River. This is what I'm talking about when I say, "Please ask me. Do you need more money for that?" So—because it's—obviously can't do the job.

Anyway, I got them together, and I said, "You've got to improve your security. You're backed up against the water. That's exactly where the terrorists will come at you." You have—if you're a powerplant, you have these big cooling things, they can drop things into that—the way for chemical companies to be blown up. I mean, we've had instances in West Virginia that have nothing to do with terrorism; they're just accidents, and they're just massively threatening. And so, they agreed to do something, and then they—this is slightly cynically put, but it's the way I look at it—they came back a year later, and they said that they'd given everybody who lets—admits people into the workspace—that is, where their cars pass through—a sidearm. Well, of course, that's the opposite side of the plant; the river is on the other side of the plant. It has nothing to do with what I'm talking about. So that what—to the extent that the private sector is willing to be helpful on something like cybersecurity, or other forms of security—always makes me just a little bit suspicious, because, as Senator Brownback said, it costs, and everybody's feeling very fragile, and everybody is very fragile, but this is—you know, this is the big one, as far as the Director of National Intelligence says. I don't know if you have any comments.

Secretary NAPOLITANO. Our interactions on the cyber side with the private sector to date have been, I think, very productive. And perhaps it's because the economic costs of a major denial-of-service attack or virus is substantial enough that there are incentives there for everyone to work together. But, this is an evolving field, it's an ever changing threat environment. And again, it's something that I think we will be dealing with for months and years to come.

The CHAIRMAN. OK. Yes, OK. Well, let—it appears that Senator McCaskill may not be coming, so I will——

Secretary NAPOLITANO. Do you want to——

The CHAIRMAN.—use her time. So just bear——

Secretary NAPOLITANO. OK.

The CHAIRMAN.—bear with me one more time.

Can you please walk me through the challenges that you face as you attempt to implement the 100-percent-scanning requirement? And I have these photographs. And, you know, I'm talking now about maritime air—I mean, water cargo containers. And some of

them, you know, they want—everybody want—in the House—wants them scanned 100 percent. You're doing it at about 5 percent, I think. And some of them—there has to be more than that, but—for example, just to pick out a Home Depot—I mean, maybe every—probably every Tuesday, at about seven different ports around the country, massive cargo containers of lumber come in. And that's predictable. It's totally predictable. So, can somebody hide something inside—a dirty bomb inside that? And does that require scanning? Then you have the—you—things are wrapped in plastic, and then they're—then they have—wrapped in metal, and they have locks. And people say, "Well, that's good," except you can blow up the locks. Well, to blow up the locks, I think, would probably be a fairly noticeable event. And so, help me understand your view of what you can responsibly, and should responsibly, do, and what you should not cost-effectively and potentially responsibly do.

Secretary NAPOLITANO. Thank you, Mr. Chairman.

I—well, I'd begin by saying that we should not believe that 100-percent scanning equates to 100 percent security. And that is because, as I mentioned before, the 100-percent-scanning rule only focuses on one method of delivery and in one place. And there are numerous methods of delivery in numerous places. And so, that is why we really have to take a more—"nuanced" is probably not the right word, but a layered, risk-based approach to these issues.

But, for example, the technology really isn't currently available. To name just one problem, we have a high rate of false positives. The logistical challenges and cost to deploy it——

The CHAIRMAN. You mean because the technology is insufficient, or because it reads and confuses?

Secretary NAPOLITANO. It reads and confuses. You have a high level of false positives. The speed of the through-port is very slow. You have lack of adequate anomaly detection. Even if you had a good technical system, recognize that you're dealing with 700 different ports around the world; having an adequately trained workforce and the maintenance of these systems is an issue.

You've got a trade issue. Many countries around the world are very—not just resistant to, but, in some respects, almost offended by the notion that we would install—you know, require this at their port, in their country. So, you have to negotiate each of those agreements separately. So, there's always the possibility of a retaliatory type of approach.

There's the additional cost to the shipping system. There was a study done recently, in the EU, that this could add as much as 10 percent to shipping costs, which, in an era of a fragile global economy, is a significant add-on.

So, I hope that gives you some picture of the difficulty that we have implementing a 100-percent-scanning rule.

The CHAIRMAN. No, it's very helpful. And I asked that question, actually, because it was so important that Senator McCaskill get here, and that, therefore, I had to tread water as best as I could.

Secretary NAPOLITANO. Oh.

The CHAIRMAN. So, she can now ask a couple of absolutely brilliant questions.

Secretary NAPOLITANO. Well, I'm glad you asked it, because I studied my answer really hard. I wanted——

[Laughter.]
Secretary NAPOLITANO.—to be able to give it to you.
The CHAIRMAN. Senator McCaskill.

STATEMENT OF HON. CLAIRE MCCASKILL,
U.S. SENATOR FROM MISSOURI

Senator MCCASKILL. Thank you, Mr. Chairman. I appreciate you holding the hearing open until I had a chance to get here. I was over in Armed Services, as we were dealing with the President's speech on Afghanistan last night, and it took a while for me to get my questioning done there.

I wanted to briefly bring up with you, Secretary Napolitano, something that I have been working on for a number of years now, and that is foreign repair stations as it relates to airline maintenance. I know this is not necessarily in your lane, but, in the long run, it needs to be on your radar—pardon the pun—because we have, increasingly in this country, turned to foreign repair stations for, not just kicking the tires, but significant maintenance and repair work for our domestic airline industry. It—FAA is—from many different hearings in this room, we have figured out we're not really sure why we certify certain repair stations but we allow noncertified repair stations to do the work. We're not really sure why we don't have the same kind of standards at foreign repair stations, in terms of background checks, in terms of perimeter security. And I bring it up to you because I think this is something that we could benefit from you—your people taking a look at this.

We had foreign repair stations doing significant work on some of our airlines in countries that were on the State Department's terrorist watch list. So, meanwhile, I—with a smile on my face, get wanded every time I get on an airplane, because I have one artificial knee, and they go through my mom's stuff, because she has two artificial knees. We have repair work, significant repair work, being done in places around the globe where I don't think the American people would be comfortable with the level of security and oversight that we're providing them.

And I wanted to bring that up to you, because it's something that I had worked on—and I know we haven't had a chance to visit about it before—but would like your reaction to that and whether or not you think that some of your obligation, as it relates to homeland security, could reach out to at least do an assessment, in your view, whether or not this is something we should be worried about.

Secretary NAPOLITANO. Well, thank you, Senator. And the foreign repair issue really reveals something which I say often, which is that homeland security does not begin at the borders of the United States. You really have to think of it in a global context and then bring it home, so to speak.

On November 18 of this year, so just a few weeks ago, we issued an actual Notice of Proposed Rulemaking on foreign repair stations, and it builds on the certification requirements that the FAA uses. But, it would require such things as making—requiring that they be open to audits by the Department of Homeland Security on a random and surprise basis. It requires certain types of recordkeeping. It requires certain types of other types of checks in the stations themselves.

The comment period on the notice, I think, closes, I want to say, the third week of January. So, it is something that has occupied our attention, and we're moving forward in that fashion.

Senator MCCASKILL. That is terrific. I know you've got to go, and I appreciate you sticking around until I got here.

I also do want to bring up—I am hopeful that you all are looking at the security clearinghouse contracting issue as it relates to a recompete. Those costs have gone up, I'm sure you're aware. A security check has risen from $3-a-head to $27-a-head. For many of our airports, that are struggling right now in this economy, it has gotten to be a very expensive proposition. And I know you all have—TSA has not gone on record yet affirming that it will open the contract to competition, but I am—wanted to go on record as saying I'm hopeful that you all will move toward a competitive contract as quickly as possible. I think this has been a sole source for way too long, and I think we're paying more than we need to pay.

Secretary NAPOLITANO. Duly noted.

Senator MCCASKILL. Thank you very much.

And thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator McCaskill.

And you have an appointment and a flight to catch. I totally thank you for being here. It's very important to us, as a committee. We respect what you're doing, and we want to be your partner.

Secretary NAPOLITANO. Thank you. Thank you, Mr. Chairman, for the opportunity to be here today.

The CHAIRMAN. Thank you.

The hearing is adjourned.

[Whereupon, at 2 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF ROBERT A. VOLTMANN ON BEHALF OF THE TRANSPORTATION INTERMEDIARIES ASSOCIATION CONCERNING THE CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM (C–TPAT)

The Transportation Intermediaries Association (TIA) is the leading education and policy organization for North American third party logistics professionals (3PLs). TIA is the only organization representing 3PLs doing business in both domestic and international commerce. With over 1200 members, TIA is the voice of 3PLs to shippers, carriers, government officials, and international organizations. As a condition of membership, all TIA members are required to sign and adhere to the TIA Code of Ethics. The members of TIA include property brokers, domestic freight forwarders, international forwarders and NVOCCs, airfreight forwarders, logistics management companies, and intermodal marketing companies. TIA is the U.S. member of FIATA (International Federation of Freight Forwarders Associations) representing more than 40,000 3PLs around the world.

TIA supports the government's effort to involve industry in the security of the supply chain. We support opening the C–TPAT Program to all companies with a significant involvement in the international supply chain willing to submit to the rigors of the program. We believe that the C–TPAT program must be run in a non-discriminatory, mode neutral manner. TIA supports mutual recognition of similar supply chain security initiatives by our major trading partners, and the steps being taken in that direction by the Department of Homeland Security. However, TIA is concerned that:

- C–TPAT is currently *not* open to all companies with a significant involvement in the international supply chain willing to submit to the rigors of the program.
- C–TPAT eligibility criteria discriminate against a significant segment of the third party logistics industry licensed by the Department of Transportation.
- C–TPAT rules do not comport with Federal law under Section 212 of the SAFE Port Act.

C–TPAT is currently not open to all companies with a significant involvement in the international supply chain willing to submit to the rigors of the program—C–TPAT excludes Department of Transportation licensed brokers and forwarders involved in cross-border trucking. The Customs and Border Protection agency (CBP) of the Department of Homeland Security (DHS) has opened the C–TPAT program to the following types of third party logistics companies: customs brokers licensed by CBP, indirect air carriers authorized by the Transportation Security Administration (TSA) of DHS, and non-vessel operating common carriers (NVOCCs) and freight forwarders licensed by the Federal Maritime Commission (FMC). CBP has *not* however, opened the C–TPAT program to brokers and forwarders licensed by the Federal Motor Carrier Safety Administration (FMCSA) of the Department of Transportation (DOT) involved in the selection and management of cross-border truck and rail carriers. This exclusion has created a hole in the security network and discriminates against a significant market sector involved in the international supply chain. 3PLs assess and maintain qualification files on thousands of motor carriers engaged in cross-border traffic. Access to this capacity through C–TPAT would allow CBP another window into the small to medium sized motor carrier industry. Yet, rather than utilize a Federal license as a requirement and develop a generic set of rules for all non-asset based 3PLs, CBP has instead staked out a confusing and discriminatory position that causes harm, confusion, and ultimately, a gap in our supply chain security network.

C–TPAT rules discriminate against a significant segment of the third party logistics industry and do not comport with Federal law. Criteria being followed by CBP for third party logistics companies do not properly reflect the nature of the industry as third party companies that select carriers, arrange for transportation and oversee the end-to-end movement of cargo in a mode neutral manner. Instead, the proposed

rules would exclude third party logistics companies that do not own equipment or take possession of freight involved in the international supply chain. If ownership of transportation assets is to be a key qualification, it is unclear why CBP has allowed into C–TPAT customs brokers, indirect air carriers, NVOCCs, and FMC licensed freight forwarders that do not meet these equipment ownership requirements, but has singled out FMCSA licensed brokers and forwarders for exclusion. In any event, the existing rules applicable to 3PLs do not comport with Federal law. The SAFE Port Act of 2006 (Public Law 109–447) states at Sec. 212 "Eligible Entities"

> Importers, customs brokers, forwarders, air, sea, land carriers, contract logistics providers, and other entities in the international supply chain and intermodal transportation system are eligible to apply to voluntarily enter into partnerships with the Department under C–TPAT.

While the Secretary is vested with the responsibility to draft rules, the existing rules are too narrow to comport with the law. DHS inexplicably has refused to admit non-asset based truck brokers "who perform duties such as quoting, booking, rating and auditing," in clear violation of the statutory mandate.

Mutual Recognition between the United States and Canada appears to continue the discrimination against segments of the third party logistics industry. It is our understanding from Canadian officials that U.S. CBP has urged Canada to bar FMCSA licensed brokers and forwarders from the Canadian Partners In Prevention (PIP) program. There are scores of Canadian companies licensed by U.S. FMCSA to operate as brokers and forwarders in the United States. These companies and their American counterparts select trucking companies and arrange for the transport of millions of trucks across the U.S.-Canadian border each year. The effort by CBP to bar these licensed companies that want to participate in C–TPAT from the C–TPAT program is discriminatory and endangers the security framework of the United States.

Mutual Recognition Must Include Mexico. U.S. DOT licensed brokers and forwarders select and manage millions of trucking movements across the U.S.-Mexican border. These companies must be able to join the C–TPAT program like all other 3PLs. As Mexico develops its own system, there needs to be mutual recognition between the U.S. and Mexican programs.

Mutual Recognition between the United States and the European Union is a good first step, but more work is necessary. TIA endorses the position and concerns expressed by the International Chamber of Commerce (ICC) with regard to C-TPAT and mutual recognition. TIA echoes the ICC's concern that mutual recognition validation is welcome, but that the need for duplicative registration processes on both sides of the Atlantic need to be eliminated.

The Customs Advisory Committee on Commercial Operations (COAC) must be opened up to 3PLs and made more representative and transparent. COAC, as the industry liaison to CBP, played a central role in CBP's consideration of eligibility criteria for third party logistics providers. For reasons unknown, property brokers were excluded from the C–TPAT process while virtually all other members of the global supply chain were included. As noted, property brokers assess and maintain qualification files on thousands of motor carriers engaged in cross-border traffic. They are in an ideal position to check on the security qualifications of those carriers as well, but COAC apparently recommended against including them in the program.

Apart from these security concerns, exclusion from C–TPAT eligibility has put property brokers, many of whom are small businesses, at an unfair competitive disadvantage in bidding against those already in the program for business from large shippers, such as automobile manufacturers, box store retailers and others who require their transportation and supply chain service providers to be C–TPAT qualified.

TIA believes that CBP may have adopted the unreasonable restrictions on 3PL participation in C–TPAT in part because it relied on faulty advice from the COAC, which is unrepresentative of the property brokerage community. Simply put, while COAC does not include property brokers, it does include members who may have a competitive interest in excluding property brokers.

TIA urges the Congress to mandate that membership in COAC must include non-asset based 3PLs. We also believe that Congress should explicitly require CBP to open the C–TPAT program to non-asset based 3PLs, as the SAFE Port Act originally intended. We would be pleased to work with the Committee in drafting legislative language to achieve those objectives.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV TO HON. JANET NAPOLITANO

Question 1. The Government Accountability Office (GAO) is releasing their report on the Secure Freight Initiative and Department's attempts to implement 100 percent scanning today. The GAO asserts that you plan to issue a blanket extension to all foreign ports. Is this correct?

Answer. The Implementing Recommendations of the 9/11 Commission Act ("9/11 Act") of 2007 mandates that, by July 12, 2012, any container loaded on a vessel in a foreign port cannot enter the United States unless it has been scanned by non-intrusive inspection technology (NII) and radiation detection equipment before being loaded onto the vessel at the foreign port. The 9/11 Act provides the Secretary with flexibility to extend the 2012 deadline in two-year increments provided two of six pre-defined conditions exist. The extension criteria within Section 232(b) permits the certification of extensions for individual port facilities, groups of individual port facilities, or all global port facilities from which U.S. bound-containers originate. The mandate to scan all U.S. bound containers with non-intrusive equipment at the overseas port of loading has now been extended by 2 years to July 2014.

Question 2. Can you please walk me through the challenges you face as you attempt to implement the 100 percent scanning requirement?

Answer. In April 2008, CBP submitted a report to Congress titled "Report to Congress on Integrated Scanning System Pilot (Security and Accountability for Every Port Act of 2006, Section 231)" and subsequent semi-annual update reports, CBP identified several technical, logistical, and diplomatic challenges associated with scanning containerized cargo at foreign ports. These challenges include but are not limited to:

- Technical
  - —Enhancing current technologies to effectively scan transshipped cargo;
  - —Sustaining equipment operations in extreme weather conditions and certain port environments (politics, cultures);
  - —Addressing health and safety concerns of host governments and respective trucking and labor unions, specifically with respect to imaging systems that use a radioactive source;
  - —Protecting data privacy concerns.
- Logistical
  - —Re-configuring port layouts to accommodate the equipment without affecting port efficiency;
  - —Persuading the foreign customs service and terminal operator to meet additional staffing requirements;
  - —Developing and implementing local response protocols for responding to alarms.
- Diplomatic
  - —Concluding agreements with partnering nations and terminal operators;
  - —Addressing the potential requirement for reciprocal scanning of U.S. exports;
  - —Addressing the sensitivities of scanning cargo within a sovereign nation.

Question 3. What lessons have you learned in implementing the pilot program since this law was enacted?

Answer. CBP reported valuable lessons learned from the 100 percent scanning pilot program as well as the significant costs associated with procuring and deploying scanning systems. These lessons learned indicate that scanning 100 percent of all U.S.-bound containers is possible on a limited scale in low volume ports processing primarily gate traffic, but it would be difficult to achieve at ports that receive transshipped containers delivered to the port facility from the waterside. CBP's reports detailed that deploying current scanning technologies at high volume and transshipment ports threaten to negatively impact port operations which would significantly delay cargo shipments, increase operating costs, and infringe on the sovereignty of foreign nations. While CBP continues to identify enhancements to current scanning technologies to strengthen cargo scanning and risk assessment capabilities, meeting the challenges of scanning 100 percent of all U.S. bound cargo by July 2012 would be difficult to achieve and the use of the extensions provided in the 9/11 Act will be required.

The April 2008 U.S. Customs and Border Protection initial Report to Congress on Integrated Scanning System Pilot can be found at *http://commerce.senate.gov/public/__files/SFIReport__PublicRelease__FINAL__Consolidated.pdf.*

Question 4. So all of us here today can understand it, please explain the Department's layered strategy for port and cargo security?

Answer. CBP implements a multi-layered, risk-based enforcement strategy designed to maximize security without causing economic disruption. This strategy encompasses the following security programs in the maritime environment:

- The "24-Hour" Manifest Rule: Advance manifest information provided 24 hours prior to lading at the foreign port;
- Container Security Initiative (CSI): Stationing CBP Officers at overseas ports to identify/examine high risk shipments;
- Customs-Trade Partnership Against Terrorism (C–TPAT): Industry partnership aimed at securing the supply chain;
- Use of Non-Intrusive Inspection (NII) Technology: Utilized for examining containers with limited impact to the port operations;
- Automated Targeting System (ATS): CBP's automated system for screening data and analyzing potential risks;
- National Targeting Center for Cargo (NTC–C): Centralized targeting center to support maritime cargo enforcement activities;
- Secure Freight Initiative's International Container Security program (SFI/ICS): Deploys scanning technology (non-intrusive imaging equipment from CBP and radiation detection equipment from Department of Energy/National Nuclear Security Administration) in support of 100 percent scanning requirement;
- Importer Security Filing "10+2": Requiring additional advanced data to enhance targeting efforts.

CBP's multi-layered, risk-based enforcement strategy relies on collecting advanced information, which is screened using automated systems and analyzed by trained personnel, to provide actionable information to CBP Officers. The screening and analysis of this information allows CBP to focus its resources on those shipments of concern, while facilitating the movement of legitimate cargo. In addition to receiving advanced information, CBP partners with industry members to enhance their own security practices throughout the supply chain. Foreign government partnerships also provide invaluable insight into potentially harmful shipments and, in some locations, have allowed CBP to deploy scanning systems to scan containers for radiation, including both imaging systems provided by CBP and radiation detection equipment provided by the Department of Energy's National Nuclear Security Administration. Finally, CBP has positioned technology at all ports of entry that serve as a force multiplier for officers in the field. Taken in combination, these layers provide meaningful supply chain security.

Question 5. Do you concur with the GAO's finding that the 100 percent scanning requirement could present challenges to the existing container security programs such as the Customs Trade Partnership Against Terrorism (C–TPAT) program and the Container Security Initiative (CSI)?

Answer. The Secure Freight Initiative (SFI), CBP's program to comply with the 100 percent scanning requirements, represents one layer of CBP's multi-layered, risk-based enforcement strategy and is not intended to replace other CBP programs and initiatives, such as CSI and C–TPAT, which represent additional layers of CBP's enforcement strategy. In the April 2008, Report to Congress referenced in Question #1, CBP included letters and correspondence from members of the local and foreign trade community as well as Foreign Governments expressing concerns regarding 100 percent scanning to include referencing the need to continue partnering with CBP in programs such as CSI and C–TPAT.

Question 6. Some foreign governments have stated that they may adopt a reciprocal requirement that all U.S.-origin containers be scanned. Would the United States be able to comply with such a mandate? Do you have any sense of what it would cost to do so?

Answer. Some Foreign Governments have suggested that they may consider adopting a reciprocal requirement that all U.S. origin containers be scanned, but no official request has been made to CBP.

Question 7. In April of this year, Acting Commissioner Jay Ahern testified that much had been done to enhance the security of cargo containers relative to other modes of transportation. He added that maritime security should not be overemphasized to the detriment of other modes of transportation. Also, he requested that the

scanning requirement be thoughtfully reconsidered by Congress. Do you believe Congress has imposed a goal on the maritime sector that is draining limited resources from other more high risk threats to our national and economic security?

Answer. A significant amount of attention and resources has been applied to the scanning of cargo containers in the maritime and land border environment which was emphasized due to the high risk threat potential of cargo containers and also to the availability of suitable commercial equipment. CBP is rapidly approaching the point where this scanning capability has been implemented for *cargo containers* that satisfies the mandates of the Security and Accountability For Every Port Act of 2006. However, challenges remain within the maritime environment surrounding bulk, break bulk and roll on roll off (RORO) shipments.

Technical challenges and resource limitations remain to find effective, suitable solutions for many other high risk vectors (*e.g.,* air cargo, general aviation, rail cargo inbound from Canada and Mexico, and between the Ports of Entry). Currently many resources have been directed toward improving the capabilities within the maritime sector that, in the future, could perhaps be better directed toward developing initial capabilities for these other high risk venues.

Question 8. I have several questions regarding DHS's chemical/biological detection capabilities for the transportation sector. First, what has the Department done to develop chemical and biological detection technologies for cargo?

Answer. The Detect-to-Protect (D2P) Triggers and Confirmers Project has been developing and testing biological detection sensor systems for high confidence detection of prioritized threat agents that have been released into the environment. These sensors are designed to be used in a variety of operational situations, with one possible deployment scenario in cargo screening environments to provide rapid warning of a semi-concealed or leaking threat, or to be used when inspecting high risk or suspicious cargo. DHS has been conducting on-going testing of these new sensors in operational environments.

DHS also has tested prototype bio-detection sensors in cargo screening environments and plans on conducting further tests as the technology matures. Currently, the device's confirmer sensor is undergoing further development and live agent testing is being conducted by the U.S. Army. DHS is also running a test of the trigger and confirmer sensors in the DC metro to see how they perform in that operational environment. Additional tests are planned for other CBP operational environments.

The goal of the Non-Intrusive Container Monitor project is to develop a sensor (or suite of sensors) that can target suspicious cargo for chemical, biological, explosives, or contraband threats, and then identify the material without exposing the public or CBP officers to the hazard. DHS released a call for proposals for a "secondary screening" technology that can address a broad range of threats—chemical, biological, explosive, and contraband—in one device, or one suite of devices that are all inter-operable.

The Autonomous Rapid Facility Chemical Agent Monitor (ARFCAM) project has been developing and testing chemical detection systems for high confidence detection of prioritized threat agents that have been released into the environment. These sensors are designed to be used in a variety of operational situations, with one possible deployment scenario in cargo screening environments to provide rapid warning of a semi-concealed or leaking threat, or to be used when inspecting suspicious cargo. These sensors have recently been evaluated in a mass transit facility.

Question 9. Do you have a deployment/implementation plan for these technologies?

Answer. CBP has devices for use in the field by scientists for chemical, explosives and hazmat detection. However, at this time there is no similar hand-held tool that can properly be used by CBP officers in the field. For biological detection CBP currently uses detection paper in the field for certain biological agents. DHS continues to work on the development of technologies for use by CBP officers in the field.

Question 10. Has the Department conducted a risk assessment of the key pathways that pose the highest risk in order to focus technology deployment once they have been determined to be operational effective?

Answer. CBP's Office of Intelligence and Operations Coordination currently is conducting this assessment and reporting the status of this work to the DHS Office of the Inspector General on scheduled intervals.

Question 11. Finally, does DHS have sufficient resources allocated in its budget for these initiatives?

Answer. DHS will continue to conduct its consolidated research program supporting chemical and biological detection systems. To date the program has yet to yield field operational devices to enhance operational detection capabilities.

Question 12. Members of Congress and the general public have significant concerns about the transportation of hazardous cargo in the maritime sector. Coast Guard protocols require vessel escorts for certain 'Especially Hazardous Cargo'. On the Ohio River Valley in West Virginia, the Coast Guard has only three small boats to protect dozens of chemical facilities and the hundreds of vessels that transport ton chemicals to them every year.

The Government Accountability Office (GAO) reported that the Coast Guard has significant resource limitations in many locations such as: a shortage of boats, a lack of qualified personnel, and unmet armament requirements, all which hinder the agency's ability to fulfill its mission requirement. Have you conducted as assessment of the assets and personnel that are needed to adequately address this core mission function? If yes, what were your findings and how can we help you? If not, could you please do so and report back to the Committee?

Answer. The Coast guard leverages intelligence, Maritime Domain Awareness and operational planning guidance to allocate assets/resources across its portfolio of 11 statutory missions to reduce safety, security, and environmental stewardship risk in the maritime domain.

On a daily basis, Coast Guard operational commanders assess all mission requirements of their respective areas of operations, including consideration of Especially Hazardous Cargo escorts, and allocate available resources to the highest priority needs.

Continued support for the Coast Guard's recapitalization programs (*e.g.,* National Security Cutter, Fast Response Cutter, Response Boat-Medium, and Maritime Patrol Aircraft), consistent with annual budget requests, is essential to sustaining the Coast Guard's ability to manage risk within the maritime domain.

Question 13. How do you guarantee that intelligence information sharing and coordination processes work properly?

Answer. A series of processes and interconnected systems ensure the intelligence components of the Department of Homeland Security share and receive critical information. Our most effective tool is the execution of a "hot wash" following an incident to document the flow of information, identify the successes, the shortcomings, and make recommendations for improvements.

Question 14. Let's take the example of port security. Can you walk me through how the Coast Guard, Customs and Border Patrol, Immigration and Customs Enforcement, the Bureau of Intelligence and Analysis, local authorities, and other DHS and U.S. Government entities share information to prevent attacks, or investigate suspicious activity?

Answer. Our processes continue to evolve and improve; in response to several recent Homeland threats, I&A created a tiger team comprising representatives from each of the Department's intelligence component, including USCIS, TSA, USCG, CBP, ICE, and our IC colleagues, called the DHS Terrorism Task Force (DTTF). The DTTF represents a significant evolution of the DHS Intelligence Enterprise by substantially increasing the thoroughness of DHS support to FBI investigations, enhancing Departmental collaboration, providing more comprehensive intelligence support to DHS leadership decisionmaking, and building toward a departmental Intelligence Enterprise. The DTTF serves as a select group of appropriate cleared individuals from across the Department. As evidenced by its activities during the past several months, the DTTF has demonstrated to our partners at the National Counterterrorism Center (NCTC) and the Federal Bureau of Investigation (FBI) that it can properly handle sensitive information while simultaneously exploiting DHS data bases to generate additional lead information. Specifically, during the threat environment from August through October 2009, the DTTF's value was demonstrated by better support to:

—The *DHS leadership* by leveraging the full benefit of DHS Intelligence Enterprise capabilities daily, and sometimes under significant time constraints. This support made for more informed DHS operational decisions in response to fast-breaking threat information. The DTTF also provided the DHS leadership for the first time a daily window into the full extent of DHS support to investigations from the perspective of the field, various Component agency headquarters, and from DHS employees embedded at the FBI and agencies of the Intelligence Community.

—The *Intelligence Community* by making informed inputs regarding the broad scope of DHS actions in response to threat information reported in the DNI Homeland Threat Task Force updates. These updates were used to brief the President and key cabinet officials about the threats and actions taken by various departments and agencies in response.

—The *National Counterterrorism Center* by illustrating the utility of expanding the dissemination of Restricted Handling material which allowed for a more Department-wide view of the threat and provided a more informed and collaborative interaction with the NCTC.

—The *nation's broader Homeland Security defense network* by ensuring that DHS outreach to our state, local, tribal, and private sector (SLTP) stakeholders was carried out in accordance with White House guidance and in close coordination with the FBI.

—The *State and Urban Area Fusion Centers* by providing greater context to the evolving threat and directing state and local partners to the information necessary for their leadership to make more informed decisions about the prevention and identification of additional threats.

- In the context of recent threat streams, DHS I&A has issued a number of bulletins and Roll Call release products to our state and local partners to sensitize them to the threat and to terrorist tactics and procedures. Zazi's activities, for example, prompted DHS to issue an advisory, Terrorist Tactics Against Mass Transit and Passenger Rail, to alert the transportation sector to possible plotting.
- In addition to bulletins and Roll Call release products, DHS I&A conducted teleconferences with State and Local Fusion Center Directors and State Homeland Security Advisors, and will conduct table-top exercises with private sector partners.

Question 15. What if actionable intelligence on an imminent threat were to come in through the wider Intelligence Community? How does that information get disseminated to these various entities, some of which have personnel who may need to act but who do not have security clearances? Can you walk me through a scenario in which the pieces of DHS along with other Federal and local authorities would share information and work together to address an imminent threat?

Answer. Actionable intelligence on an imminent threat is immediately distributed through a variety of information sharing mechanisms; including dissemination by our various IT systems, working directly with our state and local partners, our Departmental personnel in the states and with our operational components. Many of our state and local partners, as well as private sector partners have security clearances, but the Department has developed procedures to declassify critical information. For example,

- In the context of recent threat streams, DHS I&A has issued a number of bulletins and Roll Call release products to our state and local partners to sensitize them to the threat and to terrorist tactics and procedures. Zazi's activities, for example, prompted DHS to issue an advisory, Terrorist Tactics Against Mass Transit and Passenger Rail, to alert the transportation sector to possible plotting.
- In addition to bulletins and Roll Call release products, DHS I&A can conduct teleconferences with State and Local Fusion Center Directors and State Homeland Security Advisors, and can conduct table-top exercises with private sector partners.

Question 16. What about Transportation Security Administration (TSA) and other agencies, including those within DHS that it works with on a daily basis. Agencies like CBP and ICE to the Federal Aviation Administration (FAA) to local authorities? Please tell me, specifically, what you do on a daily basis to promote and ensure information sharing and cross-agency coordination on addressing threats.

Answer. The Transportation Security Administration (TSA) is an active participant in intelligence information sharing and coordination. TSA's Office of Intelligence (TSA–OI) interacts daily with members of the Intelligence Community, DHS components, governmental agencies with intelligence functions like the Federal Aviation Administration and other agencies within the Department of Transportation, Law Enforcement, and international partners.

TSA–OI is an all source intelligence office with a 24x7, 365 days-a-week intelligence watch. The Watch provides real time warning and notification for TSA/DHS Leadership, TSA Federal Security Directors, their staff, and Coordination Centers, Federal Air Marshals, and the Intelligence Community on all threats related to the transportation sector. This sector is comprised of international and domestic commercial civil, commercial cargo and aspects of general aviation. It also includes mass transit systems, passenger and freight rail, pipelines, the U.S. highway system including commercial buses and motor coaches, and a joint responsibility with United States Coast Guard for maritime issues involving ferries systems.

TSA–OI also has a professional cadre of all source intelligence analysts who provide value added intelligence analysis of transportation-related information to a broad range of TSA stakeholders in the form of briefings and written products.

To support this analysis TSA–OI has analysts embedded at the CIA, the National Counterterrorism Center (NCTC), the NSA, the FBI's National Joint Terrorism Task Force (NJTTF), and FBI's Terrorist Screening Center (TSC). TSA–OI analysts are also assigned to DHS Intelligence and Analysis and located at CBP's National Targeting Center (NTC).

TSA–OI's Field Intelligence Officer program provides intelligence support to over 25 of the Nation's busiest airports. Field Intelligence Officers (FIOs) support the Federal Security Directors and their staffs, interact with the local FBI JTTF, and communicate with state and local law enforcement and security officials responsible for transport security. While physically located at a major airport, all FIOs have regional responsibilities. FIOs are responsible for all modes of transportation. FIOs interact with Federal, State, and local aviation, modal authorities, law enforcement, fusion and intelligence centers, JTTFs, etc.

At the local port level, leveraging the Interagency concept of operations, the Coast Guard Sector works with law enforcement partners to increase and improve the sharing of actionable law enforcement information between the Coast Guard, CBP, ICE, TSA, FAA and other Federal, state and local law enforcement partners, for more efficient and effective coordinated operations and response to threats and incidents.

Coast Guard Sectors also lead Area Maritime Security Committees (AMSCs) and Harbor Safety Committees and sometimes additional locally-unique Federal/state/local/international organizations.

At the national level, the USCG Headquarters Command Center in Washington, D.C. and the Coast Guard Intelligence Coordination Center (ICC) in Suitland, MD conduct direct coordination regarding suspicious activities with DHS and other Federal partners, appropriate to the nature of the activity. Both units have 7x24 watchstanding operations.

The National Response Center (NRC), collocated with the USCG Headquarters Command Center, is the interagency Federal nexus for suspicious activities reported by critical industries in our ports and waterways. Industry reports which meet Federal Bureau of Investigation (FBI) criteria are forwarded by the NRC directly into the FBI Guardian system, where the reports are accessible by the Joint Terrorism Task Force (JTTF) units nationwide and all JTTFs have a variety of DHS members.

ICE Intel disseminates vital information to the Intelligence and Law Enforcement Communities through the production of Homeland Intelligence Reports (HIRs).

In FY 2009, ICE disseminated over 600 HIRs containing information relating to national security, Southwest Border security, transnational criminal activity, and threats to public safety. HIRs produce and incorporate information from open sources, law enforcement data bases, and classified information. They are disseminated to the appropriate parties as based on content.

Question 17. Protecting the Nation from security risks posed by the nearly 13 million small vessels that exist is a monumental task. There are parallel security threats in the general aviation sector, which has been a long unaddressed vulnerability in our aviation industry. I understand that you and Admiral Allen are preparing a revised Small Vessel Security Strategy. When will that be finalized? It is my understanding that DHS has a number of related programs to address small vessel security but they do not coordinate with each other. How will you integrate these multiple programs into one comprehensive, layered security approach?

Answer. The Small Vessel Security Strategy was published in April of 2009. The DHS Small Vessel Security Implementation Plan is expected to be released by the Department in 2010. The Plan is being developed through an integrated DHS component small vessel security working group. The small vessel security initiatives of component agencies are being coordinated to eliminate redundancies and ensure coordinated implementation actions among Federal partners.

Question 18. TSA has not conducted a national railroad risk assessment as required by the 9/11 Act. As a result, TSA has been unable to assess the potential consequences of certain proposals, such as allowing guns on Amtrak trains, on the security of the passenger rail network. What are you doing to guarantee that TSA completes the risk assessment, as required?

Answer. As required by the 9/11 Act, the Transportation Security Administration (TSA) has conducted the Transportation System Sector Risk Assessment (TSSRA), which encompasses railroads and other surface transportation modes. Through TSSRA, TSA has evaluated threat, vulnerability, and consequence in a wide range of terrorist attack scenarios for each mode of transportation. For mass transit and

passenger rail, this assessment considered more than 200 scenarios, rating threat capabilities and likelihood of execution; vulnerabilities of rail and bus systems and infrastructure; and potential consequences in casualties, property damage, and impacts on the transportation network. The resulting risk ranking enables setting of informed mitigation priorities, both across the sector and by individual mode, for collaborative security strategies, program development and resource allocations. The TSSRA is in the final stages of review at TSA.

Question 19. The Visible Intermodal Prevention and Response (VIPR) program works with local law enforcement to serve as a deterrent to potential terrorist attacks. However, a recent GAO report found that some VIPR teams do not have sufficient training or enough radios and other communication equipment to coordinate effectively with local law and surface transportation officials. What are you doing to ensure that TSA provides sufficient training and resources so that VIPR teams can help protect our transportation networks?

Answer. The Transportation Security Administration (TSA) routinely works with local transportation and law enforcement stakeholder/partners to train and familiarize TSA deployable assets that are used on Visible Intermodal Prevention and Response (VIPR) operations. Much of this training is completed at the local level and is specific to particular modes of transportation. One such example is TSA's continuing initiative to train Federal Air Marshals (FAMs) and Transportation Security Officers (TSOs) to work in mass transit environments alongside local transportation and law enforcement stakeholder/partners. Both FAMs and TSOs receive training directly from the partnering transportation authority on safety matters, the transit agency's physical structure, and specific operating procedures. TSA also sends its personnel to numerous anti-terrorism training courses that have specific application in the transportation domain.

TSA plans to develop an agency-wide VIPR specific training curriculum for all TSA deployable assets that participate in VIPR operations. In addition, TSA's Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) has developed specific VIPR law enforcement training that is instructed at its training academy and field office level.

TSA's OLE/FAMS has provided the necessary interoperability communication equipment for the 10 dedicated VIPR teams. Additionally, in Fiscal Year (FY) 2010, TSA received funding for an increase of 15 VIPR teams, dedicated to the surface domain. The FY 2010 funding provides the necessary radio communication equipment and training.

Question 20. What else can be done to improve our protection of critical infrastructure from cyber attacks and what can be done to improve public-private partnerships between government agencies and critical infrastructure providers?

Answer. The National Cyber Security Division (NCSD) within the Department of Homeland Security (DHS) engages in a wide variety of initiatives designed to improve the protection of critical infrastructure from cyber attacks. Many of NCSD's ongoing initiatives illustrate areas where NCSD is pursuing improvements to current processes and practices. Generally, however, improvements in the protection of critical infrastructure from cyber attacks could be gained from implementing appropriate security measures and effective partnerships across the Critical Infrastructure and Key Resources (CIKR) sectors. Initiatives such as the development of improved national cyber incident response, multi-directional information sharing, improved national capability and capacity to detect, prevent, respond to, and mitigate disruptions of voice and cyber communications, and increased security for CIKR industrial control systems are ready examples of areas where additional efforts will improve CIKR cybersecurity.

Question 21. What can be done to improve public-private partnerships between government agencies and critical infrastructure providers?

Answer. Public-private partnerships between government agencies and critical infrastructure providers are key to improved cybersecurity for the Nation's CIKR. NCSD works closely with private-sector representatives from each of the CIKR sectors and is actively engaged in strengthening and expanding those relationships. Partnerships are based on trust, which is enhanced through continued mutual engagement between and among public- and private-sector partners. Initiatives currently being pursued to improve public-private partnerships include: increasing collaboration with industry on key plans such as the National Cyber Incident Response Plan; integrating private-sector involvement in cyber operations centers, including the new National Cybersecurity and Communications Integration Center; expanding the services of existing cyber operations centers such as the Industrial Control Systems Cyber Emergency Response Team; and continuing to protect the Nation's CIKR networks through risk-mitigation efforts conducted in full partnership with

industry as outlined in the Information Technology Sector Baseline Risk Assessment.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BYRON L. DORGAN TO HON. JANET NAPOLITANO

Question. I understand that the Transportation Security Administration (TSA) is actively examining the current process for facilitating background checks for aviation workers in an effort to enhance competition. I fully support the principle of competition, so long as the high standards set by the current system are maintained and security is never compromised. I hope you will adequately assess the key capabilities necessary to maintain a successful process, including the ability to instantaneously determine the status of any individual worker in the system and to quickly respond to evolving TSA requirements and directives. Maintaining the highest bar for security must be your goal.

As you contemplate changes in this area, I urge you to pursue a careful and informed course that ensures:

Today's high security standards are not diminished and all vendors qualified by TSA meet the same high standards required today of the Transportation Security Clearinghouse (TSC).

Airports have the ability to select a qualified entity to provide these services at their facility.

The current TSC services, developed at no cost to the Federal Government, remain available to airports and other users without disruption.

With that in mind, I would like your answer to the following questions:

What safeguards do you have in place to ensure that the existing process and high standards are not disrupted as you pursue competition for background screening services? What safeguards will be in place to ensure that existing security capabilities are not diminished as changes in this area are implemented? Does TSA intend to require that all service providers are capable of monitoring the status of all workers it processes prior to their assumption of these services at airports?

Answer. In examining the current aviation worker screening process, a primary objective of the Transportation Security Administration (TSA) is to maintain or improve upon existing security standards and practices. TSA hopes that competition in this area will yield process enhancements and security capabilities that operationally improve aviation worker background checks. As part of this process, TSA is establishing data submission standards and will include best practices for data security. The provider(s) selected to provide aviation screening services would be expected to adhere to these standards and undergo periodic reviews.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO HON. JANET NAPOLITANO

Question 1. Madam Secretary, as you know, there is a one-hundred percent screening requirement for all cargo placed on commercial passenger flights that goes into effect next August. In some instances, meeting this mandate without causing undo economic harm is going to be challenging. Let me give you an example. In Washington State, the fresh cherry season is very short and cherries need to be picked, packed and shipped within twenty-four hours. During the season, fresh cherries are flown from SeaTac to Asian markets on anywhere between eighty to one hundred dedicated freight aircraft flights as well as in the cargo hold of numerous commercial passenger flights. To help Washington State cherry growers meet the current fifty percent inspection requirement, this summer TSA provided K–9 units to help scan the cherries shipped on these commercial passenger flights. I thank the Department for doing that. But everyone recognizes this is not a viable long term solution to meet my growers need to have fruits shipped on commercial passenger flights and TSA's need to ensure the security of our skies.

I have been told that equipment is being tested that would allow freight forwarders to scan full pallets and containers at airports before they are loaded onto planes. The availability of this technology would greatly improve the ability of Washington cherry growers to get their highly perishable product to Asian markets quickly and efficiently, and eliminate the need for dogs. What is the status of the technology and what is the status of the testing? When do you believe freight forwarders will be able to begin utilizing these scanners? To meet the one-hundred percent scanning requirement will it be possible to accelerate the rollout of these scan-

ners? If the scanning technology is not widely available by the beginning of next cherry season, will the Department continue to provide K–9 units?

Answer. Electronic metal detector technology that may offer the potential to screen individual boxes and skids (up to 40 inches by 48 inches in size), provided that no metal is used in packaging, is currently being tested in the laboratory and in the field. Testing is being conducted using as aggressive and expedited a schedule as is possible consistent with good test practices and concern for security. If testing shows that systems using this technology are effective and suitable, freight forwarders will be able to purchase and use such systems immediately upon notification of system qualification. The Transportation Security Administration (TSA) expects that notification of system qualification will be provided not later than end of March 2010, before the start of the cherry season.

Explosive detection canine units will remain an integral portion of air cargo security screening and TSA's program was expanded by an additional 35 teams in 2009. Although TSA will continue to facilitate these situations with canines as much as possible, TSA will not be able to fully alleviate the need for screening this cargo each time due to limited resources and the increased amount of cargo to be screened across the Nation once the 100 percent mandate becomes effective. Alternatively, businesses such as the cherry growers can participate in TSA's Certified Cargo Screening Program, which would permit these entities to physically search the cargo as they build it up and offer it for transport as screened cargo given all required security measures of the program are adhered to. This program is available for participation now and is being used by shippers of various time sensitive and high value goods, perishable goods or goods that require very special handling.

Question 2. Madam Secretary, roughly seventy percent of container ship traffic entering the Port of Seattle and the Port of Tacoma is discretionary. That is, only thirty percent of the contents of these containers "remain" in Pacific Northwest. The "vast majority" gets transported to points east, primarily by rail.

Washington State Ports compete with Canadian ports in Vancouver and at Prince Rupert for discretionary container traffic. Asian shippers decide where to ship to, based on price and schedule. I understand that the statutory mandate to scan all U.S. bound containers with non-intrusive equipment at the overseas port of loading has now been extended by 2 years to July 2014.

Madam Secretary, do you know if container ships bound for Western Canadian ports will have similar security requirements for in-bound containers? For example, if containers arriving in Western Canadian ports from country "A" are placed on rail and are transported across the U.S.-Canadian land border, will the U.S. security of these containers be equivalent to containers arriving at a Washington State port directly from country "A"? If that is not the case, do you think that this difference in requirements present an increased level of security risk to the U.S.? Also would this place U.S. west coast ports at a competitive disadvantage? More broadly, do you see a need to harmonize policies and practices with respect to ensuring the security of in-bound containers across North America?

Answer. CBP has developed a multi-layered process to target and examine high-risk shipments while simultaneously facilitating legitimate trade and cargo. We are accomplishing this through legislative initiatives, use of advance information, risk-management targeting systems, detection technologies, extended border strategies and the human factor.

CBP screens the data and information for all cargo containers arriving in the United States from foreign locations, regardless of the country of origin or the mode of transportation (*e.g.,* sea or rail); and closely scrutinizes and examines all shipments identified as high risk. CBP employs its layered enforcement process to thoroughly screen and ultimately examine 100 percent of the shipments that pose a risk to our country.

Question 3. Madam Secretary, the semi-submersibles vessels used by Central and South American drug-runners are typically built in the jungles of Columbia, only built for a one-way trip, and are designed to be scuttled (sunk) once either the delivery is made or the vessel is detected by law enforcement.

This is an extremely effective method for drug-runners, but is there any evidence that groups or individuals have considered using semi-submersible vessels for something other than the drug trade? Are our drug enforcement officials, law enforcement officials, and intelligence agencies actively communicating to make sure that if there is interest among terrorist groups or others for using semi-submersible vessels for things beyond drug transport, our Nation's homeland security system will pick up on that?

Answer. Available reporting indicates Self Propelled Semi-Submersibles (SPSS) are built for the express purpose of transporting cocaine from South America to off-

load sites on or near the coasts of Central America, Colombia, and Mexico. No available reporting indicates SPSS operations have occurred in U.S. territorial waters. Moreover, little to no evidence indicates groups outside the drug trade have used SPSS vessels in any capacity.

Question 4. I know that your department and the Coast Guard are working on the problem of small vessel security, and developed a Small Vessel Security Strategy in April of 2008. Semi-submersibles vessels are not mentioned in that strategy, though. Should they be, or are semi-submersibles a separate threat demanding a separate strategy?

Answer. The DHS Small Vessel Security Strategy characterizes small vessels as any pleasure or commercial watercraft regardless of method of propulsion that is less than 300 gross tons. Although there is no exact correlation between a vessel's length and its gross tonnage, a vessel of 300 GT is approximately 100ft in length. This definition was used to ensure that all potential small vessel threats, including SPSS vessels, were covered.

Question 5. Is the Department of Homeland Security currently developing a semi-submersible vessel security strategy? If not, why not?

Answer. The Department of Homeland Security is developing a submersible vessel strategy, which describes the Department's strategic approach for countering the increased usage of self-propelled semi-submersible (SPSS) vessels, as well as the potential use of self-propelled submersible (SPS) vessels (submarines) to smuggle illegal drugs.

Question 6. Madame Secretary, as you know, the 2010 Winter Olympics in Vancouver, Canada will occur this coming February. First, I want to thank you for your leadership and support in developing the 2010 Olympics Coordination Center in Bellingham and your agency's strong partnership over the last 5 years in the 2010 Olympics Security Committee. The facility is providing a location for inter-agency training, coordination, meetings, and exercises that has significantly strengthened overall preparedness in the region. It has proven its utility during the Police and Fire Games completed this summer and I know will do so once again during the upcoming Olympics. I believe the Coordination Center is capable of continued operations beyond the games with local Emergency Management and homeland security activities in the region continuing to operate out of the facility. I believe this capability is valuable for increasing the region's overall preparedness along our northern border. Madam Secretary, are you willing to work with me to see how the Department can maintain the Coordination Center as a legacy preparedness facility into the future?

Answer. The Olympic Coordination Center has proven invaluable for various events, notably: local tabletop exercises; "Gold," the largest National Level Exercise ever undertaken by Canada and a real-world event; and the World Police and Fire Games. We are looking forward to achieving the same level of success for the 2010 Olympic and Paralympic Games in early 2010. As with any facility that DHS operates, continued management of the Coordination Center will be evaluated strategically and weighed against operational and resource constraints.

Question 7. On page 42, of the April 2007 GAO report entitled "First Responders: Much Work Remains to Improve Communications Interoperability" (GAO–07–301), the GAO recommended that DHS "develop and implement a program plan for SAFECOM and other OEC interoperability programs that includes goals focused on improving interoperability among all levels of government".

Currently, are DHS entities in the field required to develop radio communications plans for specific areas of operation? If so, are these plans cross walked with the plans of all of the state, local, and tribal governments the DHS entities in the field work with on a day-to-day basis in order to identify gaps in multiple agency communications?

Answer. Currently, there is no Federal or Department-wide policy that requires Department of Homeland Security (DHS) field components to develop radio communications plans for specific areas of operation. However, the Office of Emergency Communications (OEC) does have a strong day-to-day working relationship and feedback mechanisms with State, local, and tribal governments concerning strategic planning activities. In several instances, DHS entities have developed radio communications plans for specific areas of operations. For example, the Federal Emergency Management Agency Disaster Emergency Communications Division has undertaken an extensive effort to develop 27 State, 14 Emergency Support Function, and four regional emergency communications plans. These plans provide guidelines for pre-positioning and deploying communications resources during catastrophic incidents to support emergency communications needs in the event of a loss of local and regional communications services.

DHS and its Federal, State, and local partners do work collaboratively to build and implement the national policy framework, governance structures, and operational capabilities to make the development of operational plans easier, more effective, and better integrated. These activities take into account the unique missions and geographies of DHS components, Federal agencies, and State and local agencies, as well as the varying requirements of those components for radio communications and interoperability. They include the following:

National Emergency Communications Plan (NECP)—In July 2008, DHS released the first National Emergency Communications Plan in accordance with Congressional direction. In developing this plan, DHS and OEC worked closely with stakeholders across all levels of government to develop a measurable, actionable national strategy to better coordinate and guide efforts to improve nationwide operability, interoperability, and continuity of communications across levels of government and public-safety disciplines. The NECP complements and supports overarching homeland security and emergency communications legislation, strategies, and initiatives, including the National Response Framework (NRF), the National Incident Management System, the National Preparedness Guidelines, and the Target Capabilities List. Taken together, the implementation of the goals and objectives of the NRF, NECP, and other DHS strategy documents will improve nationwide response efforts and bolster situational awareness, information sharing, and on-the-ground tactical communications.

State, local and tribal Integration—OEC has strong day-to-day working relationships and feedback mechanisms with State, local, and tribal governments concerning strategic planning activities. OEC works with the 56 States and territories, and several tribal nations, to implement existing strategic plans through statewide planning workshops and technical assistance. OEC also encourages the States, through their Statewide Interoperability Coordinators, to maintain representation by all levels of government on their statewide interoperability governing bodies and coordinate their strategic and tactical activities across all relevant partners.

Question 8. My understanding is that the majority of the State, Local, and Tribal Law enforcement agencies operating on the Olympic Peninsula utilize the UHF band for communications. I am told most Federal agencies (including DHS) operating on the Olympic Peninsula are utilizing VHF band radios for their communications. DHS communications are primarily conducted on the Department of Justice, Integrated Wireless Network (IWN)—an encrypted VHF trunking system. Operationally, CPB agents need to be able to scan the radios of State, Local, and Tribal law enforcement, to know if they need to respond to a call for mutual aid, and more generally, to maintain situational awareness . These trunked VHF radio systems cannot scan the UHF band. And here lies the problem. It is somewhat mitigated at Blaine because the CPB and local law enforcement share a common dispatch center. On the Olympic Peninsula, though, dispatchers for local law enforcement agencies and CPB are geographically dispersed which make the coordination all that more challenging. Is DHS aware of the challenges of trunking radio systems and the barriers they present to multi-agency day-to-day field communications, particularly in more rural communities?

Answer. There are two dimensions of the technical communications challenge represented in this question: (1) dealing with multiple radio technologies (trunked/non-trunked, analog/digital, proprietary/standards-based), and (2) dealing with multiple frequency bands.

The biggest technology challenge is interoperating with proprietary systems rather than standards-based systems. The only methods currently available to achieve interoperability between multiple proprietary systems or from proprietary to standards-based systems are either carrying multiple radios, or using a gateway device or audio switch technology that bridges systems together by connecting a radio or each system to the gateway.

If you are dealing with standards-based systems (*i.e.,* Project 25 (P25)), the trunked/non-trunked and analog/digital issues become much more manageable. All P25 digital radios are required to be backward compatible with analog systems. In addition, all P25 trunked radios are compatible with non-trunked P25 systems. Therefore, if an emergency responder needs to connect to multiple networks, it is recommended that they specify and purchase standards-based trunking capability in their radios and ensure that they are programmed appropriately for each network that it must operate on.

In regard to the challenge of dealing with multiple frequency bands, there are gateway devices available that can enable a UHF network to communicate with the Integrated Wireless Network (IWN), which communicates on the VHF band. For example, in the greater Seattle metropolitan area, it is possible to set up radio gate-

ways with local and state agencies via the Tri-County Radio Interoperability System (TRIS), which includes King County, Pierce County, Snohomish County, the Port of Seattle, and IWN. In areas not covered by the TRIS, interoperability switches are available and can be used to establish interoperability among disparate networks.

The IWN's trunking system equipment (*e.g.,* portables, mobiles, and consolettes) is capable of operating in both P25 trunking and conventional narrowband and conventional wideband modes in the VHF spectrum, 136–174 MHz. These radios only operate in the VHF band but some local agencies in the State of Washington operate in the VHF band as well, and if authorization is obtained, these frequencies can be programmed into the VHF equipment listed above.

Another alternative for local agencies operating in the UHF 400 MHz band or 700/800 MHz bands is a multi-band radio (MBR). The Department of Homeland Security (DHS), Science and Technology Directorate's (S&T's) MBR project hosted a short-term demo in Whatcom County and Blaine, WA, between 12 local, state, and Federal agencies in the summer of 2009 that enabled communications between UHF (400, 700/800 MHz) and VHF (138–174 MHz) bands. In preparation for and during the 2010 Winter Olympics in Vancouver, British Columbia, Canada, DHS S&T will conduct a more detailed MBR pilot in that region from January 30-March 1, 2010, to assess cross-border, rural and multi-agency emergency communications and interoperability.

Question 9. As you may know, Assistant Secretary Bersin and I, working with State, Local, and Tribal officials on the Olympic Peninsula, created the Multi Jurisdictional Task Force to improve communications between CPB and local law enforcement stakeholders on the ground regarding a range of issues that impact our northern border. The group identified a number of areas where more work is needed and made a number of recommendations. Are you aware of the Multi Jurisdictional Task Force and its short-, mid-, and long-term recommendations? How does the Department intend to follow up on these recommendations?

Answer. CBP is fully aware of the task force and the concerns that it has identified with regard to radio interoperability.

The overarching concerns are:

- The majority of the Olympic Peninsula's state, tribal and local (STL) law enforcement agencies/departments utilize Ultra High Frequency (UHF) band communications.
- Most Federal agencies operating on the Olympic Peninsula are utilizing Very High Frequency (VHF) band, while incorporating digital encryption or trunking.
- Within DHS, communications are primarily conducted on the Department of Justice, Integrated Wireless Network (IWN), an encrypted VHF trunking system.

In response to these concerns, the Office of Border Patrol and the Office of Information Technology are actively working with STL law enforcement partners on the Olympic Peninsula and have developed a path forward which addresses the short-term, mid-term, and long-term goals of radio interoperability.

The short-term goal is to establish an effective radio communications capability prior to the beginning of the 2010 Winter Olympic and Paralympics Games. To date the following actions have been taken:

- Clallam County Sheriff's Department has loaned five mobile radios, which were installed in Border Patrol vehicles to assist in radio interoperability until a long-term solution is implemented.
- Blaine Border Patrol Sector has loaned 15 portable (hand held) VHF radios to Clallam County SO and other local law enforcement agencies (LEA) to improve interoperability on the Olympic Peninsula.
- An ACU–1000, which provides a single UHF/VHF radio channel for emergency radio interoperability on the Olympic Peninsula has been installed at the Port Angeles Border Patrol Station.
    - The ACU–1000 will be utilized during the 2010 Olympic Games and beyond, until a long-term interoperability solution can be implemented.
- The Clallam County Sheriff's Department has a Mobile Command Center (MCC), which has an ACU–1000 installed in it, and can also be utilized in the event of a large scale emergency.

To address interoperability concerns after the 2010 Winter Olympic and Paralympic Games, and until a long-term communications solution can be developed and implemented, the following courses of actions are being pursued:

- Continue to utilize short-term options beyond the Olympic timeframe, until a long-term solution can be implemented.
- Continue reassessing communications interoperability based upon the needs of the Olympic Peninsula law enforcement community.

In looking forward, CBP is actively pursuing a long-term communications solution for the Olympic Peninsula by taking the following actions:

- Implement the CBP communications modernization effort in the Olympic Peninsula.
  - Procure dual band VHF/UHF portable radios so that Border Patrol Agents can communicate directly with other STL law enforcement officers at the lowest level.
  - This technology will not be available until as late as 09/2010.
  - Procure and install UHF capable vehicle mounted radios in CBP law enforcement vehicles so that Federal law enforcement can communicate "car to car" with STL partners.

Procure and install dual-band VHF/UHF base station radios to increase communications between departments, vehicles, and law enforcement personnel.

Question 10. Madam Secretary, one issue this Committee examined in 2007 with respect to the preparedness and coordination of first responders across multiple jurisdictions and multiple agencies is interoperable communications. It is still a work in progress. Washington State's long-term approach is to use Radio over Internet Protocol (RoIP). The Olympic Public Safety Communications Alliance Network (OPSCAN) consists of over 40 local, state, Federal, and Canadian public safety agencies, including DHS. OPSCAN has a fairly extensive footprint in my state's Region 1.

One key advantage with using RoIP is that first responders, when responding to an incident, in principle, can use their existing radios. And with budgets being stretched as they are, it is especially hard for smaller communities, especially where first responders are volunteers, to afford purchasing new radios. Another approach the Department is looking at to achieve interoperability is to develop multiband radios.

First, the Department has been looking at the use of radio over IP and VOIP for interoperable communications for several years. What do you consider to be the barriers for technology's widespread adoption by first responders?

Answer. Although based on Internet Protocol (IP) standards, Voice Over IP (VoIP)/Radio Over IP (RoIP) technology is not always interoperable because it can be implemented in a number of different ways by manufacturers. As a result, there is no guarantee that one manufacturer's equipment will successfully interface with another's, even though they may both use the same standards. To address these interoperability gaps, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) is assisting in the development of VoIP specifications.

The Olympic Public Safety Communications Alliance Network (OPSCAN) network uses a product from a Seattle-based company that implements a Bridging Systems Interface (BSI) to help provide connectivity between the agencies involved in the program. The BSI is an interoperability specification developed by DHS S&T in partnership with the Department of Commerce's Public Safety Communications Research (PSCR) program. DHS S&T and PSCR worked with emergency responders as well as this company and others during the development of this specification. This specification is currently implemented by 12 companies in their commercially available products and is a big step toward addressing the technical barriers to implementing interoperable RoIP solutions. Further, DHS is producing a BSI Best Practices Guide aimed at administrators and technicians that will provide guidance on procuring and establishing interoperable communications using the BSI.

The largest barriers remaining for widespread implementation of RoIP as an interoperability connectivity technology are related to demonstration and knowledge dissemination. Most RoIP demonstration projects, including OPSCAN, use a single-vendor solution to provide the RoIP connectivity. A specific effort toward demonstration projects that use multi-vendor RoIP equipment would be very helpful toward demonstrating the viability of the technology. Further, more effective means of disseminating the successes and challenges of implementing such a system would also be helpful.

Question 11. What more needs to be done to evolve OPSCAN and OPSCAN-like networks from a pilot project into a system for everyday use, and is that something the Department is willing to consider pursuing in partnership with the State of Washington?

Answer. The largest remaining barriers for widespread implementation of Radio Over Internet Protocol (RoIP) as an interoperability connectivity technology are related to technology demonstration and knowledge dissemination. Most RoIP demonstration projects, including the Olympic Public Safety Communications Alliance Network (OPSCAN), use a single-vendor solution to provide the RoIP connectivity. A specific effort toward demonstration projects that use multi-vendor RoIP equipment would be very helpful toward demonstrating the viability of the technology. Further, more effective means of disseminating the successes and challenges of implementing such a system would help in the development of products such as best practices, lessons learned, and user guides that provide emergency responders and other stakeholders with a better understanding of the benefits and challenges they are likely to encounter when implementing a technology.

Question 12. Does the Department intend to conduct a pilot of the Bridging Systems Interface program in Washington State's Region 1 during the time of the Winter Olympics to see whether it does improve interoperability under real world conditions?

Answer. Because the Olympic Public Safety Communications Alliance Network (OPSCAN) network uses the Bridging System Interface (BSI); the BSI will be piloted by proxy in any activities that involve the OPSCAN network for the Winter Olympics. DHS will work with its partners in Washington State to obtain any after-action reports from these activities to help validate the application and use of the BSI in real-world scenarios.

Question 13. The Department is currently conducting a series of Multiband Radio Project pilots. How will the Department know if the pilots are successful and what would be the next steps?

Answer. The Department of Homeland Security (DHS), Science and Technology Directorate (S&T) is initiating Phase III of a three-phase, multi-band, portable radio (MBR) project. Phase I was the laboratory testing phase, which included emergency response agencies conducting limited in-house laboratory testing in their radio facilities and laboratory testing conducted by the Department of Commerce Public Safety Communications Research Program located at the National Institute for Standards and Technologies in Boulder, Colorado Phase II was the test-demonstration phase that included an evaluation of the prototype radios by emergency response agencies during training exercises and some use in the field. Phase III is the actual pilot testing by multiple agencies across the Nation using pre-production prototype radios. Upon completion of the pilots, participating practitioners will be interviewed by an independent party to help understand how well the pilot achieved its goals and how well the product met the expectations of emergency responders. All three phases of the project include the documentation of results, which will be compiled into a detailed final report on the mission impact and the improvement and enhancement of radio communications interoperability.

DHS S&T undertook the MBR project to equip emergency responders with the unprecedented capability of operating across the entire range of public safety radio bands. Another goal of this project was to encourage additional manufacturers to develop portable radio equipment of similar capabilities with a future goal of seeing those manufacturers develop and produce a similar mobile, multi-band radio for installations in vehicles and mobile command centers (higher power version). These efforts have sparked industry's decision to invest in similar technologies; thus far, DHS has identified a total of four different companies that have developed or are currently developing a version of a MBR.

Looking ahead, software-defined radio technology could provide an alternative solution that is expected to advance to a cognitive radio technology in the future. A cognitive radio solution would not be restricted to specific radio bands allocated to emergency response agencies and could therefore access any available unused/authorized spectrum available within the region. Ongoing research and development initiatives are underway but there are numerous regulatory issues as well as technical issues that must be resolved before this type of technology will be available.

Question 14. Our borders and homeland security systems are being tested every day by illegal drug smugglers. The illegal drug trade uses every tool at its disposal, transporting massive quantities of drugs by land, air, and sea. For example, international drug smuggling between Washington State and Canada is often done covertly using helicopters. And in the eastern Pacific Ocean, drug smugglers are now using increasingly sophisticated and hard-to-detect semi-submersible vessels.

If drug smugglers are able to transport tons of drugs into our country each and every day, what does this say about our Nation's ability to detect and stop the smuggling of people and weapons for other purposes like terrorism? Do you believe that use of increasingly sophisticated transport methods like helicopters and semi-

submersibles are a potential threat to homeland security? Wouldn't an increased crackdown against international drug smuggling by agencies like the Coast Guard also have a side-benefit of strengthening our Nation's anti-terrorism presence?

Answer. Your question identifies critical issues. It is the primary mission of the Department to prevent terrorist attacks within the United States and to reduce the vulnerability of the United States to terrorism.

The illicit drug trade is a vast and lucrative enterprise. While it is a practical impossibility to stop all illicit trafficking, DHS commits nearly four billion dollars a year to support the national drug control program, including approximately three billion dollars for drug interdiction. DHS works in collaboration with its partners in the Departments of Justice, Defense, and State, and with our partner nations to most effectively target our intelligence, interdiction, and investigations to mitigate the threat posed by illicit drug trafficking to the homeland.

I share your concerns that terrorist organizations may employ the means and methods of drug traffickers to move terrorists or weapons of mass destruction into the United States. One example of the Department's vigilance to reduce the vulnerability to these threats is the response to self-propelled semi-submersible (SPSS) vessels. As the threat posed by SPSS vessels developed, the Department proactively sought legislation to designate the operation of SPSS vessels without nationality as illegal and a threat to the security of the United States. The resulting Drug Trafficking Vessel Interdiction Act established civil and criminal penalties for persons using, navigating, or operating SPSS vessels without nationality.

In the last part of your question, you ask if "an increased crackdown against international drug smuggling by agencies like the Coast Guard also have a side-benefit of strengthening our Nation's anti-terrorism presence?" While the reallocation of resources to support one mission may result in a "side-benefit" to another mission, it is important to understand possible detrimental consequences—direct and indirectly—of any reallocation of resources on efforts to battle terrorism. DHS is committed to identifying the appropriate allocation of resources amongst its various missions to maximize the ability of the Department to mitigate threats to the homeland, and particularly those posed by terrorists and weapons of mass destruction.

Question 15. Given ongoing concerns about cost, schedule, and performance issues with major acquisitions such as Deepwater and SBInet, what progress has DHS made and what more can be done to ensure that DHS acquisitions stay within cost, on schedule, and perform as intended?

Answer. DHS has developed a comprehensive approach that establishes acquisition management standards and oversight. Directive 102–1, *Acquisition Management* was issued November 2008 establishing acquisition program processes and formal acquisition review boards (ARBs) that oversee major departmental programs.

During an ARB, the program manager (PM) summarizes program status relative to cost, schedule and performance. The ARB serves as a forum to assess acquisition program progress and bring essential issues to the Acquisition Decision Authority (ADA). The ARB also performs a staffing function to recommend, along with the PM, decisions and courses of action for the ADA who exercises final authority for the ARB. Once each ARB is completed, DHS documents it in a formal Acquisition Decision Memorandum (ADM) and actively monitors the completion of assigned ADM action items. DHS also tracks program manager certifications and ARB progress and approval. Since the directive was issued, over fifty ARBs have been held, of which five were with SBI and six with USCG programs. Additionally, ten USCG Acquisition Program Baselines (APBs) were approved by the Departmental ADA.

To complement the ARB process, Component Portfolio Reviews were implemented. This process, jointly executed by the Component and the Department, supports management of the Component's acquisition portfolio and strengthens Departmental governance and oversight. These reviews also provide insight as to systemic acquisition risks across the Department.

DHS has designated six Component Acquisition Executives (CAEs) who are responsible for program execution at their respective Components. The CAE can chair decision meetings for specific programs as delegated by the Under Secretary for Management (USM) who is the Department's Chief Acquisition Officer (CAO).

Seven Independent Expert Program Reviews (IEPRs) have also been conducted on programs of senior leadership interest that have cross cutting areas pertinent to acquisition. In particular, an IEPR for SBInet was conducted in FY 2008 and the USCG National Security Cutter (NSC) in FY 2009.

In the future, DHS will continue to expand the oversight and governance efforts listed above, as well as taking actions to strengthen the acquisition enterprise (such as analyzing the adequacy of program staffing for its major program portfolio).

Question 16. Improving the acquisition workforce has been noted as a key acquisition management priority at DHS for the past several years. What steps has the department taken to build and sustain a sufficient, capable, and properly trained workforce to support DHS's acquisition portfolio? What additional actions does the department plan to take to strengthen its acquisition workforce?

Answer. To improve DHS's ability to effectively manage its current initiatives and plan strategically for our acquisition work force, the Department has taken the following steps:

1. We established an interim working definition (positions within the Department that devote a minimum of 50 percent of time and responsibilities to performing acquisition duties) of the acquisition workforce that more accurately reflects the number of employees performing acquisition-related functions to guide current efforts, while continuing to formally add career fields to the definition. Currently, DHS has established two acquisition workforce career fields and one acquisition workforce assignment specific specialty: (1) Contract Officers and specialists, (2) program managers, and (3) contracting officer's technical representatives. Further, the Department has initiated the expansion of the acquisition workforce to include Test and Evaluation, Logistics, Systems Engineering, and Program Cost Estimating.

2: We have leveraged the successful execution of the Department-wide Acquisition Professional Career Program (APCP). This program serves as one initiative to address the Department's shortage of acquisition professionals by recruiting highly motivated and intelligent individuals into entry level acquisition career fields. In addition to growing the Department's acquisition talent, the program also serves to develop a pipeline of future acquisition leaders and to facilitate the goal of establishing the culture of One DHS.

The APCP program began in 2008 and since that time has grown to 109 participants. By the end of FY 2010 program will grow to 200 positions and in FY 2011 the program expects to reach its full end strength of 300 positions. Since 2008, the program has focused on recruiting contract specialists, but, in September 2009, DHS hired its first "technical cohort" that consisted of 13 participants to include acquisition program managers and systems engineers. In Fiscal Year 2010 and 2011, the program will expand to other acquisition career fields to include Business Cost Estimators, Information Technology Specialists, and Logisticians. This program is expected, once fully implemented, to add up to one hundred fully trained and certified new acquisition professionals to the DHS Acquisition workforce every year to offset losses from retirements and transfers to non DHS agencies.

3. We have developed a comprehensive implementation plan to execute the existing DHS acquisition workforce initiatives, including:

- Developing and executing a Department-wide Acquisition Workforce Human Capital and Succession Plan in accordance with the FY 2008 National Defense Authorization Act.
- Continuing the successful use of the direct hire and reemployed annuitant hiring flexibilities to expedite hiring and to fill critical vacancies.
- Implementing the centralized hiring concept through assumption of the lead role in all Department-wide acquisition-related vacancy announcement postings.

4. The Chief Procurement Officer has coordinated with the Department's Chief Human Capital Office to establish a joint process for coordinating future acquisition workforce planning efforts with the components for the purposes of informing Department-wide planning efforts.

5. Improving the collection and maintenance of data on the acquisition workforce by the following:

- Assessing what additional data on current acquisition workforce members, such as attrition data, would help inform workforce planning efforts and then developing a strategy to collect that information.
- Expanding the collection of acquisition workforce data from the appropriate component point of contact to include all positions that DHS determines to be acquisition-related.
- Conducting an assessment of options for creating systems to maintain comprehensive acquisition workforce data and selecting the appropriate system.

6. The Office of the Chief Procurement Officer, Acquisition Workforce Branch is responsible for providing career development training for the entire DHS ac-

quisition work force. Future acquisition workforce growth and succession requirements as well as competition for talent between other agencies and the components has raised concerns that reliance on these outside training sources will not satisfy DHS's long-term needs to train and retain employees. To that end, DHS has established a centralized DHS Acquisition Workforce Training and Certifications Offices to meet the expanding requirements and has increased throughput of students completing certification training to fill operational positions within the DHS headquarters and Components.

Since its establishment in 2007, the Acquisition Workforce Branch (AWF) Training Team has relied on various sources for the development and delivery of acquisition-related training as a means to satisfy its certification training and continuous learning requirements. The goals of these offices are to:

- Develop and execute a centralized acquisition workforce training program comprised of certification, targeted, and continuous learning developmental training opportunities.
- Further expand, in addition to Contracting, Program Manager, and Contracting Officers Technical Representative certification programs, the DHS definition of the Acquisition Workforce by developing the Test and Evaluation career field by the end of the 2009 calendar year and begin drafting the Logistics and Systems Engineering career field certification programs.
- Publish a DHS course catalog and acquisition training curriculum.
- Implement a DHS wide online central registration and certification system.

The Acquisition Training Office was established near the end of the 2007 Fiscal Year. In its first full training year, approximately 1,200 seats were available to be allocated for training. The FY 2010 training program is projected to offer over 8,000 training seats. This represents almost a 1000 percent increase in training throughput capacity in two short years.

Student training and certification figures;

FY08 Training Catalog and Calendar
- 14 = Total number of titles in FY08 catalog
- 47 = Total number of classes scheduled
- 1,200 = Approx. number of seats available for all of FY08
- 820 = Approx. number of students enrolled

FY09 Training Catalog and Calendar
- 42 = Total number of titles in FY09 catalog
- 293 = Total number of classes scheduled
- 7,900 = Approx. number of seats available for all of FY09
- 6,785 = Approx number of students enrollments processed to date

FY10 Proposed Catalog and Calendar
- 52 = Total number of titles in proposed FY10 catalog
- 283 = Total number of classes proposed to be scheduled
- 8,500 = Approx. number seats available for all of FY10

FAC–C Certifications Issued (Levels I, II, and III)
- FY2007: 163
- FY2008: 450
- FY2009: 478

DHS Program Management Certifications Issued (Levels I, II, and III)
- FY2007: 279
- FY2008: 517
- FY2009: 694

COTR Certifications Issued
- FY2007: 2,199
- FY2008: 2,281
- FY2009: 2,116

Average Cost per Student

Through the use of consolidated training contracts and a centralized reservation system, the Acquisition Workforce Training Team decreased the average training cost from approximately $2,000 per student to approximately $250 per training seat. Further consolidation efficiencies will continue to drive cost lower while standardizing the acquisition workforce training requirements to meet the departments' needs.

Question 17. The Coast Guard Authorization Act for Fiscal Years 2010 and 2011, of which I am the lead sponsor, includes numerous provisions to strengthen the

Coast Guard, including a significant overhaul of the Coast Guard's acquisition programs. I strongly believe that we need to end the misuse of lead systems integrator approaches to acquisition and build a system of serious accountability. How important is it for the Coast Guard Authorization bill to be enacted this Congress? Can you please comment on the importance of the bill's Coast Guard acquisition reforms to help protect taxpayers, end wasteful spending, and provide the Coast Guard with the assets it needs to protect our Nation?

Answer. Enactment of an Authorization Act for the Coast Guard is essential. I believe that such legislation must include provisions—such as section 301 (Vice commandant; vice admirals) of S. 1194—that would enhance the efficiency and effectiveness of the Coast Guard and, by extension, the safety and security of the United States.

The Department and the Coast Guard remain committed to adopting and implementing the acquisition reforms contained in S. 1194—the evidence of which is the significant department-wide improvements already implemented in acquisition policy, processes, and execution. I believe that such reforms could strengthen and solidify these improvements; thus, these reforms are important, not only to the Service, the Department, and the Government, but ultimately to the American people.

Broadly speaking, I believe that acquisition reform, particularly those for an individual component, must not have a deleterious effect on either the Department's ability to manage and oversee component acquisition activities or my authority to unify departmental policies and practices. I stand ready to assist in whatever manner to ensure the swift enactment of an Authorization Act for the Coast Guard, and I look forward to working with you, this Committee, and Congress to ensure that these acquisition reforms are included—specifically, in a manner consistent with departmental policy and guidance.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO HON. JANET NAPOLITANO

Question 1. Two years ago, Congress acted to require one hundred percent scanning of all shipping containers coming to the U.S. However, right now we are only scanning less than 5 percent of all U.S.-bound containers and the GAO found that one hundred percent screening has not been achieved at even one port. Can you identify any concrete, specific improvements in cargo scanning that have been made by this Administration since January?

Answer. CBP's Secure Freight Initiative (SFI) is the Agency's program to deploy scanning and imaging systems overseas to meet the 100 percent scanning mandate of the 9/11 Commission Recommendation Act. SFI has produced positive results in identifying needed improvements to current technologies to enable CBP to detect anomalies in containerized shipments via imaging systems. CBP continues to work with the vendors of imaging systems to integrate these upgrades into the next generation scanning systems.

SFI has scanning systems deployed at the Ports of Qasim, Pakistan; Southampton, United Kingdom; Puerto Cortes, Honduras; and Busan, Korea and anticipates being fully operational at the Port of Salalah, Oman in April 2010. SFI operations at these ports continue to provide CBP with data to enhance risk targeting, the ability to test system and scanning technology enhancements, and experience and lessons learned to evaluate potential additional locations that would strategically enhance CBP's targeting efforts.

Question 2. The 9/11 Commission highlighted the importance of securing mass transit and passenger rail. The 9/11 Act we passed in 2007 set deadlines for securing our surface transportation networks, but TSA has missed many of these deadlines. How much longer will it take for TSA to meet these deadlines, including the comprehensive risk assessment and national security strategy for the rail sector that is due this month?

Answer. The Transportation Security Administration (TSA) is currently working on a set of risk assessments in response to several congressional mandates and Government Accountability Office recommendations. These reports, including the freight rail risk assessment and national security strategy required by section 1511 of the Implementing Recommendations of the 9/11 Commission Act of 2007, are expected to be completed and submitted to the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB) in the near future. TSA is also working on a Notice of Proposed Rulemaking (NPRM) that would require employee security training program requirements for surface modes of transportation. These include freight railroad carriers, public transportation agencies (including rail mass

transit and bus systems), passenger railroad carriers, over-the-road bus operators, and motor carriers transporting Highway Security-Sensitive Materials.

Question 3. Worldwide, mass transit and passenger rail have been frequent targets of terrorist attacks. Just last week a terrorist bombing of a Russian train resulted in the loss of twenty six lives. Yet our transportation security efforts have focused almost exclusively on aviation. What immediate steps is this Administration taking to protect the millions of Americans who travel by mass transit and passenger rail?

Answer. The Administration is advancing a multi-faceted strategy to protect passengers traveling in mass transit and passenger rail systems through the following priority areas:

- *Rail Transportation Security Rule*—The Transportation Security Administration (TSA) issued a final rule to enhance the security of our Nation's rail transportation system, which included requirements for intercity, commuter, and short-haul passenger train service providers and rail transit systems. See 73 FR 72130, November 26, 2008.
  - The rule codifies the scope of TSA's existing inspection program and requires regulated parties to allow TSA and Department of Homeland Security officials to enter, inspect, and test property, facilities, conveyances, and records relevant to rail security.
  - The rule also requires that regulated parties designate rail security coordinators and report significant security concerns.
- *Security Training Programs for Surface Mode Employees*—Pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007, TSA is developing a Notice of Proposed Rulemaking (NPRM) that would require employee security training program requirements for surface modes of transportation.
  - The NPRM would cover public transportation agencies (including rail mass transit and bus systems) and passenger railroad carriers, as well as freight railroad carriers, over-the-road bus operators, and motor carriers transporting Highway Security-Sensitive Materials (HSSM).
  - The NPRM will propose minimum elements for the training programs addressing security awareness, terrorist behavior recognition, and threat and incident prevention and response for frontline employees.
- *Protect High Risk Assets and Systems*—Targeting grant investments through the Transit Security Grant Program for Fiscal Year (FY) 2009 and the American Recovery and Reinvestment Act (ARRA) of 2009, totaling nearly $525 million, for expanded operational capabilities and enhanced protection of critical infrastructure.
  - Of note, nearly $78 million of the $150 million awarded under ARRA specifically focuses on expanding capabilities for visible, unpredictable deterrence through the funding of dedicated law enforcement anti-terrorism teams, including explosives detection canine teams and mobile explosives detection screening, and reducing risk in transit systems.
  - TSA augments these growing capabilities with deployment of Visible Intermodal Prevention and Response (VIPR) teams. Through a joint planning process between TSA, the transit or rail agency's law enforcement and security team, and local law enforcement officials, the VIPR team's composition and activities are tailored to the needs of the participating system. VIPR teams provide a range of capabilities to enhance detection and deterrence in mass transit and passenger rail, including surveillance detection, behavior observation, mobile explosive trace detection for random bag inspections, explosives detection canine teams, specialization to resolve suspected explosive devices, and other visible, random, and unpredictable security activities. During 2009, TSA conducted more than 1,050 VIPR operations with mass transit and passenger rail systems across the Nation.
  - Amtrak and TSA have jointly planned and executed large-scale, integrated rail security operations in the Northeast Corridor, which encompasses the largest concentration of passenger rail services and highest volume of passengers in the Nation. The most recent operation unified law enforcement officers from 149 departments in an unannounced surge to 157 passenger rail stations from Richmond, VA, to Portland, ME, during morning rush hours of September 9, 2009. These operations have provided a foundation for recurring, joint security activities between Amtrak and law enforcement partners throughout the Northeast Corridor. TSA coordinates with mass transit and

passenger rail systems in a risk-based approach in other metropolitan areas to advance similar approaches.

- *Elevate the Security Baseline*—Pursuing continuous improvement through comprehensive security assessments under the Baseline Assessment for Security Enhancement (BASE) program, use of the results to inform security enhancement priorities, follow-up to assist in security enhancement with the assessed agencies, and broad sharing of the most effective practices identified in the assessments.
  - TSA surface transportation security inspectors conducted more than 40 BASE assessments during 2009.
  - In December, TSA distributed an updated compilation of smart security practices drawn from the assessment results to law enforcement chiefs and security officials in mass transit and passenger rail agencies. This compilation consists of 80 smart security practices, many of which focus on regional partnerships, random security patrols, sweeps, and surges, and intelligence and security information sharing, and training and public awareness. Its specific purpose is to foster communication among security professionals in mass transit and passenger rail nationally with the specific objective of expanding adoption of these most effective practices, tailored as necessary to each agency's operating environment.
- *Build Security Force Multipliers*—Expanding informed, capable "eyes and ears" for security through targeted grants awards during FY 2009 for employee security training, anti-terrorism exercises, and public awareness campaigns, and specially trained and equipped anti-terrorism law enforcement teams and technological systems to enhance detection and deterrent capabilities. TSA augments these capabilities through focused support programs, including the following conducted during 2009:
  - Intermodal Security Training and Exercise Program (I–STEP), designed specifically to enhance capabilities of regional security partners to work collaboratively to enhance capabilities to prevent acts of terrorism through joint workshops conducted over a period of months and a regional table top exercise.
  - Bomb Squad Response to Transportation Systems—Mass Transit, which uses training and scenario-based exercises to expand regional capabilities to respond to a threat or incident involving a suspected explosive device in mass transit and passenger rail systems by placing bomb technicians from law enforcement forces in a transit or rail system's operating area in situations requiring coordinated planning and execution of operations to identify, resolve, and, if appropriate, render harmless improvised explosive devices.
  - Employee Vigilance Campaign, which, under the theme of "NOT ON MY SHIFT," employs professionally-designed posters to emphasize the essential role that mass transit and passenger rail employees play in security and terrorism prevention in their systems. Adaptable templates enable each transit agency to tailor the product to its operations by including the system's logo, photographs of their own agency's employees at work, and quotes from the senior leadership, law enforcement and security officials, or frontline employees. The unified Federal/local message is conveyed by the inclusion of the Department of Homeland Security seal alongside the agency's logo.
- *Lead Information Assurance*—Employing the full range of capabilities to ensure timely delivery of intelligence and security information, at classified and unclassified levels, to mass transit and passenger rail security officials.
  - During 2009, a joint DHS Office of Intelligence and Analysis, TSA Office of Intelligence, and Federal Bureau of Investigation effort provided classified intelligence and analysis presentations to mass transit and passenger rail security directors and law enforcement chiefs in more than 20 metropolitan areas simultaneously through the Joint Terrorism Task Force (JTTF) network's secure video teleconferencing system. These briefings, held in July and December 2009, advance two key strategic objectives—providing intelligence and security information directly to mass transit and passenger rail law enforcement chiefs and security directors and enhancing regional collaboration by bringing these officials together with their Federal partners to discuss the implications for their areas and coordinate to implement effective security solutions. The briefings will continue on approximately a quarterly to semi-annual basis, with additional sessions as threat developments may warrant.

- At the unclassified level, TSA periodically produces and disseminates Mass Transit Security Awareness Messages that address developments related to terrorist activity and tactics against mass transit and passenger rail.

- *Expand Partnerships for Security Enhancement*—Engaging continuously with senior executives, law enforcement chiefs, and security managers for mass transit and passenger rail agencies; State and local government officials, law enforcement, and emergency responders; and Federal partners to foster regional security coordination and to integrate the spectrum of available resources for enhanced deterrent and response capabilities.
  - In the Department, the Office of Inter-Governmental Programs oversees this outreach, ensuring close coordination at all levels of government on security enhancement activities and actions to address a threat or incident. TSA has made outreach to, and cooperation with, governmental and industry partners the central element of its security enhancement activities.
  - In 2009, TSA, with its Federal partners, most notably the Federal Transit Administration (FTA) and the FBI, held two joint meetings with the Mass Transit Sector Coordinating Council (SCC), which represents corporate and employee interests through representatives from the American Public Transportation Association (APTA), the Community Transportation Association of America (CTAA), Amalgamated Transit Union (ATU), Amtrak, and individual transit agencies representative of the community in system size and geographic spread, as well as representation of business organizations providing support services to the public transportation industry. These sessions streamline the coordination process between government and the transit industry, helping to advance a partnership in developing and implementing security programs.
  - TSA also consulted extensively with the Transit Policing and Security Peer Advisory Group (PAG), which consists of law enforcement chiefs and security directors from 15 mass transit and passenger rail agencies of varying size, types of services, and locations. The collective expertise and diverse experiences of the Group provide invaluable practical context to TSA's policy and program development and implementation, assuring that developing security enhancement programs and initiatives align with operational realities in mass transit and passenger rail systems. Ten teleconferences and one joint meeting were held with the Group during 2009.
  - Finally, TSA and DOT's Federal Transit Administration (FTA) jointly sponsored two Transit Security and Safety Roundtables, which brought together law enforcement chiefs, security directors, and safety directors from the Nation's 50 largest mass transit and passenger rail agencies and Amtrak with Federal security partners. In a workshop format, the participants discuss specific terrorism prevention and response challenges and work collaboratively in developing effective risk mitigation and security enhancement solutions. The Roundtables also enabled the transit agencies safety and security officials to share effective practices and develop relationships to improve coordination and collaboration.

Question 4. Maritime workers are required to go through background checks and obtain biometric I–D cards to gain access to our ports. Now that the deadline for workers to obtain these TWIC cards has been met, TSA must focus on deploying technology that can be used to accurately read the cards. How long will it be before our ports have the technology in place to read TWIC cards?

Answer. As required by the Security and Accountability For Every Port Act of 2006, DHS will implement final reader requirements through the rulemaking process. DHS intends to issue regulations that require owners and operators of MTSA regulated vessels and facilities to have and use TWIC readers in access control systems. The law requires DHS to conduct a card reader pilot program to test the business processes and technology required to deploy transportation security card readers. The pilot also will examine operational impacts for vessel and facility owners and operators.

Currently there are a total of 24 participants in 9 different geographic locations representing a broad sampling of MTSA-regulated facility and vessel operations (EOA/ST&E start dates included):

- Port Authority of Brownsville, TX (early April 2009).
- Watermark Cruises, Annapolis, MD (early May 2009).
- Magnolia Marine, Mississippi (mid-May 2009).
- Staten Island Ferry (early June 2009).

- Clipper Navigation, Seattle, WA (late August 2009).
- Port Authority of New York and New Jersey (planned February 2010).
- Port Authority of Los Angeles (planned February 2010).
- Port Authority of Long Beach (planned January 2010).
- APM Terminal, Portsmouth, VA (planned January 2010).
- Exxon/Mobil, Baton Rouge, LA(planned January 2010).
- Shell Norco, Norco, LA (planned January 2010).

The statute further requires that any final TWIC card reader rule be consistent with the findings of the pilot program. DHS intends to issue a rule after the final TWIC card reader pilot program report is made public, incorporating the data and conclusions into the rule and its supporting analyses. This will ensure the public has ample time to review both the rule and the report before DHS implements a final rule.

At this time there is no requirement for ports to use readers and the TWIC reader pilot program has not been completed. Once a final rule is published, DHS anticipates a phase-in period at the ports with the reader technology.

Question 5. In its last budget submitted to Congress, the Administration requested two-hundred and fifty million dollars for port security grants, a one hundred fifty million dollar cut from the program's authorized level. As the President formulates his budget for next year, will you recommend that he request the full authorized amount of funding for the Port Security grant program?

Answer. Section 112 of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) amended 46USC § 70107 and authorizes $400,000,000 for the Port Security Grant Program (PSGP) for Fiscal Years (FY) 2007 through 2011.

Although there was a reduction in the President's budget between FY 2009 and FY 2010, the PSGP was appropriated at its full authorized amount for FY 2009 and received an additional appropriation of $150,000,000 through the American Recovery and Reinvestment Act of 2009, providing a total of $550,000,000 for the program.

Further, while the SAFE Port Act establishes a maximum amount for PSGP, other factors including the ability of grantees to absorb additional funding affect our ability to allocate funds responsibly and effectively.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CLAIRE MCCASKILL TO HON. JANET NAPOLITANO

Question 1. I realize that your agency is not directly responsible for inspection or overseeing foreign repair stations. But what is your view on how we certify and inspect foreign repair stations? Does the lack of regular inspections of foreign repair stations raise security concerns for your department? Aren't proper inspections and review also paramount for aviation security so that we have a better handle on the process and people involved in maintaining airplanes?

Answer. The Transportation Security Administration (TSA) published a Notice of Proposed Rulemaking (NPRM) on November 18, 2009, which proposes to issue regulations to improve the security of Aircraft Repair Stations as required by Public Law 108–176: The Vision 100—Century of Aviation Reauthorization Act of 2003. The NPRM proposes to establish requirements for aircraft repair stations to adopt and implement a standard security program, and to comply with security directives issued by TSA. This rule also proposes to codify the scope of TSA's existing inspection program and to require regulated parties to allow TSA and Department of Homeland Security officials to enter, inspect, and test property, facilities, and records relevant to repair stations. The comment period for the NPRM was extended to February 19, 2010.

Question 2. I'm aware that putting in security measures for the airline operations has been a significant challenge because of the diversity of aircraft, airports and operations across the country. I'm aware that there are increased background checks for pilot training. What about for airline mechanics? What can be done to check the backgrounds of mechanics at foreign repair stations? Is there any good way to track this?

Answer. The Transportation Security Administration's (TSA) proposed security regulations will require repair stations certificated by the FAA under 14 CFR part 145, to adopt a security program that will include the measures by which the repair station verifies the employment history of its employees and conducts background checks to the extent permitted by the laws of the country in which the repair station

is located. TSA will use the inspection process to make sure that the verification measures listed in the security program are adequate.

Question 3. Regarding the sole-source agreement with the American Association of Airport Executives (AAAE) to process security data for airport workers, are you planning to compete this contract when it expires in October 2010? If not, why not? It seems clear this sole-source justification is, in the nicest terms, a stretch: We are requiring a simple transactional service—about 4 secure e-mails to be exact—and there are plenty of other players in the field. Isn't this a no-brainer? In this economic climate, how can we not be doing everything in our power to get the best value for our already struggling airports?

Answer. In examining the current aviation worker vetting process, a primary objective of the Transportation Security Administration (TSA) is to maintain or improve upon existing security standards and practices. In furtherance of this objective, TSA is currently establishing data submission standards and data security requirements. TSA expects that multiple companies will qualify to meet the submission and security requirements. TSA is supportive of a model that promotes competition and airport choice and is currently evaluating several options that would achieve this. TSA anticipates that competition and airport choice in this area will yield process enhancements and security capabilities that operationally improve aviation worker background checks. TSA plans to engage industry in the first quarter of CY 2010 regarding its plans.

Question 4. You've had almost a year now to get a handle on the contracting environment at DHS. Do you know about how many other sole-source contracts like this exist? What's your plan to root out the ones that are not mission-critical and promote full and open competition across the Department?

Answer. While securing the Homeland through the acquisition of products and services is essential to our mission, executing contracts that represent good business is a priority as well. This includes maximizing competition and small business opportunities. We believe that the practices we have instituted in past years, coupled with new initiatives being implemented in FY2010, provide a strong mitigation strategy for reducing and/or eliminating the use of inappropriate sole source contracts.

A summary of our recent achievements and our key initiatives in the area of competition are discussed below.

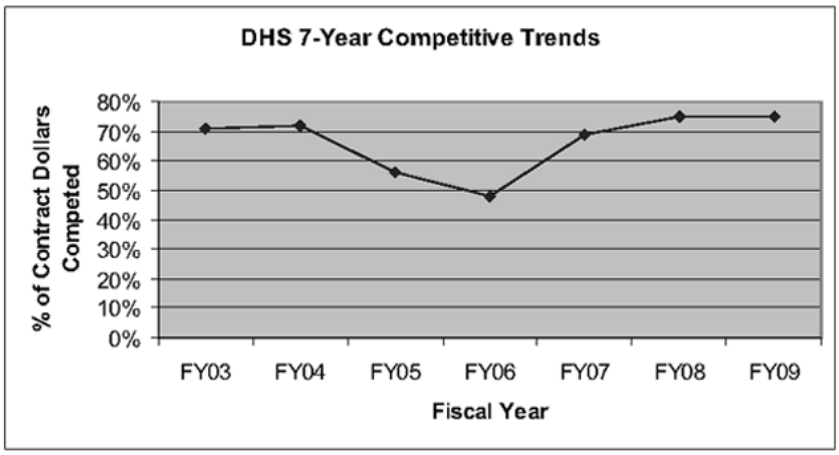
I. Competition at the Department of Homeland Security

The strength of DHS's Competition Advocacy Program is reflected in continuing improvement in the Department's level of competition. As indicated in the table below, Fiscal Year (FY) 2007 marked a recovery by DHS to pre-Katrina levels of competition. Further in FY 2008 and FY 2009 DHS achieved a level of competition equaling or exceeding 70 percent, well above the Government wide average of 64 percent.

Seven out of eight DHS Components met or exceeded their FY 2009 competition goals, and six out of eight DHS Components achieved a competition rate (in terms of competitive obligations) of 70 percent or greater.

DHS Summary Competition Data: Fiscal Years 2003–2009

Fiscal Year	Percentage of Contract Dollars Competed	Competed Dollars
FY03	71%	$2,771,342,335
FY04	72%	$5,116,950,676
FY05	56%	$5,945,514,066
FY06	48%	$7,353,642,377
FY07	69%	$8,144,115,845
FY08	75%	$10,208,340,211
FY09	76%	$10,130,114,603



Source: FPDS–NG, FY 2009 Data as of 11/30/2009.

II. Competition Program Monitoring and Oversight

The Chief Procurement Officer (CPO) and the DHS Competition Advocate monitor competition data as reported to the Federal Procurement Data System on a monthly basis. Mid-year reports are provided to the Chief Procurement Officer and to Heads of the Contracting Activities regarding year-to-date competitive accomplishments versus established goals. Corrective action plans are requested of Components with mid-year goal/achievement gaps greater than 10 percentage points.

In addition to monitoring Component competitive accomplishments versus competitive obligation goals, progress related to two new metrics will be monitored as part of the Competition Advocate's monthly, quarterly, and mid-year reports beginning in Fiscal Year 2010. These new metrics, reducing by 10 percent the percentage of noncompetitive and one bid contracts, are being added consistent with Office of Management and Budget (OMB) Memorandum M–09–25, *Improving Government Acquisition,* dated July 29, 2009, and Office of Federal Procurement Policy (OFPP) memorandum *Increasing Competition and Structuring Contracts for the Best Results,* dated October 27, 2009. As part of this effort, the Office of the Chief Procurement Officer has established individual goals for each component and is providing monthly updates to each component on their progress to date.

DHS is also involved in several post-award internal reviews of noncompetitive contract awards. The DHS oversight division of the Office of the Chief Procurement Officer recently completed a review of sole source awards made during the period of April 1, 2008 through March 31, 2009. The purpose of this review was to determine whether DHS components are awarding noncompetitive contracts in accordance with the provisions at Federal Acquisition Regulation (FAR) Part 6.3, the Homeland Security Acquisition Regulations (HSAR), the Homeland Security Acquisition Manual (HSAM) and DHS acquisition policies and guidance. Also considered was a focus on the components' use of good business judgment and adequate supporting rationale. The final report for this review, including identification of opportunities for improvement and associated recommendations, will be issued in February, 2010.

Furthermore, in accordance with DHS appropriations requirements, the DHS Office of Inspector General is directed to audit and report annually on contracts awarded during the previous Fiscal Year through other than full and open competition to determine compliance with applicable laws and regulation. In October 2009, the DHS Office of Inspector General began conducting simultaneous audits of DHS competition for FYs 2008 and 2009. The reports for both FY2008 and 2009 are anticipated to be issued in February, 2010. In addition, the Government Accountability Office (GAO) recently opened an engagement assessing the extent of noncompetitive contracting, including sole source, in the Federal Government's procurement of goods and services (GAO Code 120850) to include review of the Department of Homeland Security Competition Program.

III. Policies and Processes

The DHS competition policy conforms with that of the Federal Acquisition Regulation and the Homeland Security Acquisition Manual. OCPO Regulatory Advisories and Acquisition Alerts provide DHS Components with accurate and timely information regarding new regulatory, data collection and reporting, and procedural requirements affecting Federal, Department wide, and Component competition programs. On October 1, 2009, the third edition of the HSAM was issued containing comprehensive and updated policy guidance related to competition. Included in the HSAM are a new comprehensive DHS Market Research Guide, an expanded and revised Acquisition Planning Guide, and a Guide for Justification and Approval for Other Than Full and Open Competition (including the requirement to post noncompetitive J&As to FedBizOpps.gov).

In accordance with FAR 6.5 and Homeland Security Acquisition Manual (HSAM) 3006.5, annual Procuring Activity Competition Advocate competition reports are submitted to the DHS Competition Advocate. The reports describe Component accomplishments over the past Fiscal Year and plans for the upcoming Fiscal Year including those for increasing competition, the acquisition of commercial items, challenging barriers to competition and commercial item acquisition, and initiatives that ensure task and delivery orders over $1,000,000 issued under multiple award contracts are properly planned and issued. Component competition reports are reviewed and used to support compilation of the DHS Competition Advocate Report to the Senior Procurement Executive and the Office of Federal Procurement Policy. Instructions for preparing FY 2009 Procuring Activity Competition Advocate Reports integrates requirements associated with OMB Memorandum M–09–25, *Improving Government Acquisition,* DHS implementing instructions dated October 14, 2009, and OFPP memorandum *Increasing Competition and Structuring Contracts for the Best Results,* dated October 27, 2009.

IV. Awards, Incentives, and Outreach

In July 2007, the DHS Competition Advocate established the DHS Competition and Acquisition Excellence Awards Program as a means of renewing and increasing acquisition workforce interest in competition and related innovative procurement practices by recognizing and rewarding individuals and teams for outstanding contributions to the enhancement of competition and the use of innovative and best procurement practices. Thirteen nominations were received from across the DHS organization during the award program's inaugural year. Seven teams and individuals were selected for recognition, their efforts collectively resulting in estimated cost avoidance/cost savings of over $5.2 million. In a July 18, 2008 memorandum, the Office of Federal Procurement Policy (OFPP) cited the DHS FY 2007 Competition and Acquisition Excellence Awards Program as an example for agencies considering establishment of programs to recognize employee contributions to improving competition. Six out of eight DHS Components submitted nominations for the DHS FY 2008 Competition and Acquisition Excellence Award. Two individuals, one contracting activity, and three teams were recognized for outstanding results in competition and the use of innovative and best practices. The DHS Competition and Acquisition Excellence Awards Program call for nominations recognizing FY 2009 accomplishments was issued on December 4, 2009.

In numerous cases, including but not limited to the DHS Competition Program, issuance of revised acquisition policy or regulations is accompanied by specialized training provided to Components. For example, in anticipation of implementation of the interim FAR rule on the public disclosure of Justification and Approval (J&A) documents for noncompetitive contracts (FAR Case 2008–003), Justification and Approval development, review, and posting training was provided to 75 ICE participants in two 90-minute sessions on February 12 and 17, 2009.

The DHS Chief Procurement Officer hosts an annual DHS Industry Day in Washington, DC to provide a forum to better communicate DHS requirements and increase competition and use of commercial items by sharing information with Federal contractors and other business representatives interested in DHS contracting and subcontracting opportunities.

V. Summary

We believe that our established policies, continued monitoring of component progress, upfront and post award reviews, and proven management commitment provide a strong deterrent against and timely identification of potentially inappropriate sole source contracts. DHS's focus on its Competition Advocacy Program through closer coordination with Components, expanded Department wide policy, tailored training, recognition programs and enhanced oversight has resulted in a robust program in which the Department takes pride. The FY 2009 level of competi-

tion, at 76 percent, is a testament to the Competition Advocacy Program's success. DHS is committed to building upon this foundation by continuing to strongly implement our current initiatives and seeking new initiatives to best promote full and open competition across the department.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO HON. JANET NAPOLITANO

Question 1. As you can see, there is a great deal of confusion about what the policies are and how they should be implemented. In order to clarify the current WBI policy, please answer the following: If a passenger walks up to a WBI machine, realizes what it is, and tells a Transportation Security Officer that he does not want to go through the WBI screening, what is the correct procedure for the TSO to follow?

Answer. If a passenger gets in line for advanced imaging technology (AIT), formerly referred to as whole body imaging, screening without being directed by the Transportation Security Administration (TSA) to do so and then realizes that he or she is in the wrong line, TSA will allow that passenger to undergo walk-through metal detector screening. If TSA directs a passenger to the AIT for screening and the passenger then refuses, TSA will conduct a pat down of the passenger as an alternative to the AIT.

Question 2. If a TSO directs a passenger to a WBI machine because it is the shortest line, and the passenger states that she wants to go through a metal detector, what is the correct policy for a TSO to follow?

Answer. This will be treated as a passenger opting out of advanced imaging technology screening, and the passenger will be required to undergo a pat-down search.

Question 3. If there are both metal detectors and WBI machines being used as primary screening devices at the same checkpoint, do passengers who go through the metal detector without setting it off receive any secondary screening, such as a pat-down?

Answer. A passenger undergoes screening via the primary screening device as directed by the Transportation Security Administration (TSA). For instance, if a Transportation Security Officer (TSO) directs a passenger to advanced imaging technology (AIT) screening, that passenger will undergo the AIT screening standard operating procedures (SOP). If a TSO directs a passenger to the walk-through metal detector (WTMD), that passenger will undergo the WTMD screening SOP. A passenger who does not alarm the WTMD may receive a pat down if random screening protocols are being conducted at that time or if the passenger is wearing bulky clothing that the TSO believes could conceal a non-metal prohibited item.

Question 4. If a secondary pat-down is not mandatory for all passengers going through a metal detector at check points with both WBI and metal detectors, how does this prevent terrorists from simply choosing to go through a metal detector?

Answer. Passengers who go through the walk-through metal detector may receive a pat down, which is conducted to detect non-metallic threat items. A pat down may be conducted on a random basis or if the passenger is wearing bulky clothing that the Transportation Security Officer believes could conceal a non-metallic prohibited item.

Question 5. TSA stated policy—Passengers who do not wish to utilize this screening will use the walk-through metal detector and undergo a pat-down procedure to ensure they receive an equal level of screening. I do not believe these are acceptable options—either go through a machine that allows a TSO to see under a highly invasive image of the passenger or have a TSO give a passenger a full pat-down. What steps is TSA taking to accommodate passengers who have legitimate concerns that either option is an unreasonable privacy violation?

Answer. The Transportation Security Administration (TSA) has evaluated the privacy implications of the advanced imaging technology and screening process, and has incorporated features that effectively protect the privacy of the individual. TSA has provided the greatest level of choice consistent with the need to provide adequate security. TSA has determined that threats to the aviation domain do not remain static and are currently evolving to include non-metallic threat objects and liquids (*e.g.,* explosives) carried on persons. Given the known risk, TSA cannot accommodate passengers who are unwilling to undergo screening.

Question 6. In October 2008, TSA released a Privacy Impact Assessment for Whole Body Imaging. That assessment outlined many of the policies TSA would use with WBI machines to protect passenger's privacy. Would you support a follow up report, either by GAO or the DHS Inspector General, to assess whether those poli-

cies have been followed and that they adequately protect passenger privacy? Would you support stricter guidelines from Congress on how TSA should safeguard passenger privacy at airport screenings?

Answer. The Transportation Security Administration (TSA) would welcome a review by the Government Accountability Office (GAO) or the Department of Homeland Security Inspector General to assess whether the policies outlined within the Privacy Impact Assessment have been followed. TSA has welcomed and considered input on ways to improve the protection of passenger privacy consistent with its underlying security mission, but believes existing privacy frameworks adequately safeguard passenger privacy at airport screenings.

Question 7. Members of the general aviation community have expressed concerns about TSA's Large Aircraft Security Program (LASP) proposed rulemaking. My understanding is that TSA is already addressing these concerns by issuing a supplemental Notice of Proposed Rulemaking (NPRM). Could you share your view on how DHS should engage and work with stakeholders from the general aviation community when developing and promulgating aviation security requirements?

Answer. The Transportation Security Administration (TSA) is in the process of developing a Supplemental Notice of Proposed Rulemaking (SNPRM) to address general aviation security. The SNPRM will take into account our security partner input gathered during the public comment period. Based on this input, TSA anticipates that the proposal in the SNPRM will provide an effective and feasible security program for the general aviation community to implement, while maintaining an appropriate level of security.

In Spring 2009, TSA implemented a new stakeholder outreach strategy. This strategy includes monthly stakeholder teleconferences, the designation of TSA representatives for various regions of the United States to increase outreach capabilities to non-trade association stakeholders, and the future establishment of a subworking group under the Aviation Security Advisory Committee. This strategy bolsters TSA's industry/stakeholder communications framework and forms the foundation for current and future interactions with the stakeholder community on the development of general aviation security policies and programs.

Question 8. As you may know, Sandia and Los Alamos National Laboratories operate the National Infrastructure Simulation and Analysis Center (NISAC) for the Department of Homeland Security. This Center has provided important consequence analysis of the impact on critical infrastructure from threats ranging from terrorism to natural disasters. The work of NISAC has been important in the national prioritization of infrastructure and our response to issues such as H1N1. Have you considered using NISAC to analyze and prioritize the consequences of a cyber attack on the U.S. infrastructure? If not, will your Department explore how NISAC can assist in this important area of national security?

Answer. The National Cyber Security Division (NCSD) met with representatives of the National Infrastructure Simulation and Analysis Center (NISAC) to discuss potential areas of support for the Information Technology (IT) sector but determined that NISAC's work does not fit with planned IT sector activities. Currently, NCSD's needs in this area are met through other means; however, NCSD will continue to consider NISAC for future activities. For cross-sector cybersecurity work, NCSD receives support from Idaho National Laboratory and will receive new support from RTI International. Additionally, NCSD is under contract with the Software Engineering Institute/Carnegie Mellon University to conduct a study on cyber interdependencies across critical infrastructure and key resources; and with Sandia National Laboratories to assess the risks associated with control system components that have long manufacturing lead times or are only manufactured overseas. The first part of this study will look at the energy and water sectors and is intended to determine if the Nation needs a "critical spares" mitigation plan. NCSD plans to expand to other sectors in 2010. This effort addresses a deliverable assigned to the Department as part of Initiative 10 of the Comprehensive National Cybersecurity Initiative.

Question 9. In the hearing, you discussed the fact that good border policy is complex, balancing trained personnel, technology, and infrastructure, and must account for the differences in types of border (terrain, etc.) along both the northern and southern borders. Over fifteen years ago, Sandia National Laboratories conducted an archival mile-by-mile border study for INS that resulted in technology and infrastructure recommendations. Has that study been updated and does a similar study for the northern border exist? If not, will you consider working with Sandia National Laboratories to update the southern border study and to conduct a study of the northern border?

Answer. Since the Sandia National Laboratories study was completed, CBP has since developed an internal planning process which replaces the need for studies involving resource deployment strategies for infrastructure and technology enhancements. As part of the most recent congressionally mandated fence effort, CBP was required to develop Analysis of Alternatives (AoA) to determine if a fence was the most viable solution with consideration to operational effectiveness and cost. Subsequent to the fence effort, H.R. 2638 was passed directing CBP to conduct an AoA for all tactical infrastructure construction projects funded under Border Security Fencing, Infrastructure and Technology (BSFIT) appropriations. CBP has complied with this law and uses AoAs as the basis for tactical infrastructure and non-SBInet related technology deployment decisions along the northern and southern borders. The AoA solutions are determined by Field Commanders with engineering, environmental and real estate support provided by the CBP Office of Administration.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK BEGICH TO HON. JANET NAPOLITANO

Question 1. Tourism is one of our Nation's greatest renewable resources, yet overseas tourists coming to the U.S. have declined since 9/11 and have not yet recovered. Secretary Napolitano, would you be supportive of creating a Tourism Liaison within DHS to coordinate and interact with the travel and tourism industries?

Answer. I have designated the Private Sector Office led by Assistant Secretary Douglas Smith to work closely with the travel and tourism industry. We would welcome your support for more resources to enhance our capabilities to address tourism. We agree with you that tourism is a vital part of our Nation's economy. On October 1, 2009, I met with private sector leaders from the travel and tourism industry at a meeting hosted by U.S. Representatives Roy Blunt (R–MO) and Sam Farr (D–CA) where we discussed how the travel industry can work more collaboratively with the new Administration to improve the industry's future and strengthen the American economy. On October 22, 2009, I met with CEOs from the travel and tourism industry where I emphasized the shared responsibility between the private sector and DHS for protecting our Nation. For all private sector related issues, Assistant Secretary Douglas Smith and his office serve as the contact point. In the Homeland Security Act of 2002, the Private Sector Office was designated as advisor on the impact of the Department's policies, regulations, processes and actions on the private sector and will continue this work.

Question 2. While we can all acknowledge Transportation Security Officers and other front-line DHS personnel primarily serve a security function, their interaction with the traveling public has inescapable customer service aspects. Just as it has been demonstrated that law enforcement personnel are most effective when they treat citizens with respect, the performance of DHS security employees might be improved with a less-adversarial, more passenger-friendly approach. Do you believe DHS should provide additional customer service training to frontline security and transportation personnel to help increase their people skills and provide for a more open and welcoming environment for our international visitors and domestic travelers?

Answer. The Department of Homeland Security (DHS) continues to develop training for frontline security personnel that enables them to assess risks posed by travelers and control the environment to better secure transportation. Our training also directs our Transportation Security Officers to treat the traveling public with respect during any security procedure. For example, TSA is now developing its training to strengthen technical skills as well as skills to promote passenger understanding of the screening process.

Question 3. After the September 2001 terrorist attacks, Anchorage International Airport (ANC) was one of several airports required by the Transportation Security Administration (TSA) to invest in Explosive Detection Systems (EDS) with the understanding the TSA would reimburse the airport for at least 75 percent of the allowable costs. After installation of the EDS was complete the TSA determined there was insufficient funding and withdrew its commitments to reimburse ANC, as well as several other airports.

Congress tried to address this issue with passage of the Implementing the Recommendations of the 9/11 Commission Act of 2007, which clarified airports should be reimbursed by the TSA for eligible past costs (Public Law 110–53, Section 160). ANC has still not been reimbursed because installation of the EDS was completed before implementation of this Act. Secretary Napolitano, what will you do to address the commitment for reimbursement originally made by the TSA to airports such as ANC?

Answer. The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110–53, Section 1604) required TSA to create a prioritization schedule inclusive of airports that have commenced projects and incurred eligible costs in anticipation of receiving reimbursement. TSA uses a risk-based schedule that focuses first on those airports with sub-optimal solutions to ensure the most effective security solutions are in place for screening checked baggage.

Competing priorities such as recapitalization of equipment that is reaching the end of its useful life and completion of optimal solutions have also precluded TSA from acting on reimbursement requests.

Question 4. The United States' Arctic border used to be impenetrable, locked in ice for most of the year. A warming climate is changing this scenario, with expectations that the Arctic Ocean will be substantially ice free during summer months in 20 years. Recent summers have already seen an increase in cruise ship and marine cargo traffic in these waters and this increase is expected to expand as the ice pack withdraws.

Secretary Napolitano, what do you see as the security implications of an ice-diminishing Arctic? What does Congress need to do to respond to these concerns? Do you support investment in the needed infrastructure such as aircraft facilities, vessel monitoring systems, better communications, icebreakers, and other needs to maintain a full time national presence in the Arctic?

Answer. NSPD–66/HSPD–25, *Arctic Region Policy,* January 2009, affirms our Nation's broad and fundamental interests in the Arctic and guides the Department of Homeland Security's current operational activities in the region. As the Arctic becomes more critical to the U.S. and global economies and our national and homeland security posture, NSPD–66 notes that it is imperative that the U.S. maintain the operational ability to:

- Control U.S. borders and areas under our national jurisdiction;
- Protect against all kinds of attacks across and from the Arctic;
- Increase Arctic maritime domain awareness;
- Protect the global mobility of U.S. vessels and aircraft and freedom of navigation and overflight under the principles of customary international law;
- Ensure the operational security of the maritime transportation system;
- Address hazards in the Arctic, including response to environmental disasters and search and rescue requirements; and
- Carry out all required military activities in the region, including strategic sealift.

NSPD–66/HSPD–25 requires the heads of Executive Departments and Agencies with responsibilities relating to the Arctic region to work to identify future budget, administrative, personnel, or legislative proposal requirements to implement the elements of the U.S. Arctic Policy. Working with the Congress and OMB, the Department will continue to seek to integrate the operational requirements and goals of NSPD–66/HSPD–25 with its other budget imperatives.

DHS and the Coast Guard will continue to further define the requirements for infrastructure support in this region. Toward this end, the Coast Guard has contracted for a "high latitude study" to assist in determining mission and infrastructure requirements to properly carry out its eleven statutory missions in the Arctic (and Antarctic) now and in the future. Currently, DHS has all of the statutory authorities it requires to implement the tasks outlined in NSPD–66/HSPD–25 and any other legislation imposing mission requirements applicable to the Arctic region. Finally, the Department and the Coast Guard continues to support U.S. ratification of the 1982 Convention on the Law of the Sea.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KAY BAILEY HUTCHISON TO HON. JANET NAPOLITANO

Question 1. In response to my question regarding border wait times, you responded that wait times at CBP crossing facilities on the Texas-Mexico border had actually decreased 12 percent. However, these figures only account for time spent inside the CBP facility and not the long lines waiting to get in. At nearly all border crossings in Texas, bridge operators and owners and local officials consistently tell me that wait times outside CBP facilities can be 30 to 90 minutes or longer for freight and/or passenger vehicles. The reason they have provided to me is that there are not enough CBP staff to operate all available lanes or to expand hours of operation at congested crossings. How do you plan to supplement your measurement

methods to reflect wait times outside facilities and to gauge the necessary staffing levels, number of open lanes and operating hours to decrease total wait times at CBP crossing facilities to shorter and more acceptable levels?

Answer. In addition to recording and tracking our transaction time of processing vehicles and travelers through primary checkpoints, CBP also reports on wait times at our land border ports of entry. These wait time reports include the wait times outside CBP facilities. While in FY 2009 in Texas CBP saw an improvement in peak wait time averages of 14 percent compared to FY 2008, wait times outside CBP facilities can often be 30 to 90 minutes or longer. Wait times are publicly reported on the CBP web page *http://apps.cbp.gov/bwt/*.

Wait times are an important concern for travelers and those involved with or affected by international travel and trade. A proactive approach to increasing public awareness of our mission responsibilities plays a vital role in helping raise public awareness and understanding of factors influencing wait times. Before anticipated high volume holiday traffic and high anticipated wait times our field offices provide public advisories. Additionally, our CBP port managers are directed to prepare in advance of peak travel periods and staff accordingly. Many of our locations have wait times as a result of traffic volume exceeding port infrastructure limitations. Impediments include insufficient access roads, road infrastructure, buildings, bridges, and tunnels which are beyond the control of CBP. Additional focus is necessary to address these issues in many locations.

With regard to measurement methods, CBP is planning to coordinate a test of land border wait time measurement technologies (loops, GPS, RFID, Bluetooth, video imaging, etc) later this year, with the objective of enhancing wait time measurements. Although the initial tests will be on the northern border, the analysis and best practices identified will improve our methodologies.

CBP prepares a Workload Staffing Model (WSM), which is used as a decision-support tool to assist in strategically determining CBP officer manpower requirements. The Port of Entry volume, number of lanes, and workload factors at each POE are drivers in this model. The WSM is consulted as OFO applies its Resource Allocation Model (RAM) process, which integrates operational and budgetary decisions on where available resources will go. Wait times are also used as a factor in helping to prioritizing funding of infrastructure construction projects.

Last year, in the commercial truck environment, CBP implemented extended hours pilot programs in both El Paso/Ysleta and Laredo/World Trade Bridge. These pilot programs were discontinued after about 6 months, as there was very little volume during the additional hours.

CBP continues to address staffing and infrastructure issues and continuously work toward improving wait times.

Question 2. The Transportation Worker Identification Credential, known as TWIC, has been in development for 7 years, and although the card has been issued to over 1.4 million transportation workers, without the installation of the necessary card reader systems at our Nation's ports, the TWIC is currently an expensive "flash pass". When does DHS anticipate that TWIC will be a viable and complete security program?

Answer. DHS has issued over 1.4 million Transportation Worker Identification Credentials (TWIC) leading up to and since the national compliance date of April 15, 2009. All personnel requiring unescorted access to secure areas of the Maritime Transportation Security Act of 2002 (MTSA) regulated facilities and vessels, and all mariners holding Coast Guard issued credentials are required to possess a TWIC. Prior to receiving a TWIC, all personnel are vetted to verify they do not pose a potential security threat to the maritime transportation system. The TWIC is currently used as a proof of identification and furthers DHS's multi-layered approach to the safeguarding of our Nation's ports and critical maritime infrastructure by ensuring only vetted individuals have unescorted access to secure areas.

DHS intends to issue regulations that will require owners and operators of MTSA regulated vessels and facilities to have and use TWIC readers in access control systems. MTSA requires DHS to conduct a card reader pilot program to test the business processes and technology required to deploy transportation security card readers. The pilot will also examine operational impacts for vessel and facility owners and operators. The pilot, currently underway at multiple facilities and vessels around the country, is critical to informing future rulemaking on the operational impacts to affected facility and vessel owners and operators. MTSA also requires that any final TWIC card reader rule be consistent with the findings of the pilot program.

DHS intends to issue a proposed rule in Spring 2011, after the final TWIC card reader pilot program report is made public this winter. Data, supporting analyses, and conclusions from the report will be incorporated in the proposed rule. DHS has

a legal obligation to permit the public to comment on the methodology and data underlying any final rule. This will ensure the public has ample time to comment on both the proposed rule and the report before DHS publishes a final rule.

A final rule requiring ports to use readers could publish the following year assuming there are no significant issues raised during the comment period. An ample phase-in period is anticipated after publication.

Question 3. TSA has told the Committee that it is considering harmonizing its credentialing programs with the aim of greater flexibility and fee fairness for transportation workers. Given the disparity of the various credentialing programs across DHS, how and when does the Department plan to achieve this interoperability, so that a truck driver carrying hazardous materials into ports or across borders would not have to apply for two or three separate DHS programs, each with its own fee structure and background check?

Answer. The Transportation Security Administration's (TSA) Office of Transportation Threat Assessment and Credentialing (TTAC) is leading an Integrated Project Team (IPT) to harmonize security threat assessments and fees across all modes of transportation. To the extent possible, TSA is developing a universal framework to harmonize the nature of the threat assessment processes and security fee schedule.

The universal framework is being developed in alignment with the TTAC Infrastructure Modernization initiative, an initiative to enhance TSA vetting and credentialing programs that affect the security of all critical transportation sectors. TSA is modernizing its business processes and systems to improve and maintain the effectiveness and efficiency of transportation security threat assessments.

Regulated TSA populations will incrementally transition to the universal modernized platform as quickly as possible consistent with government operational requirements and Federal rulemaking procedures. Therefore, the harmonization of background checks and associated user fees will be possible after the necessary regulatory changes have become final, the supporting infrastructure has been modernized, and all populations have been transitioned from current acquisition contracts to the new platform. While TSA is finalizing an integrated schedule, it is expected that the universal framework will become effective during the second or third quarter of 2012, and that TSA programs will be incrementally added to the framework thereafter. Note that this framework is for TSA regulated programs only, and will not cover CBP, ICE, Secret Service and many other DHS programs.

It is DHS's goal, in partnership with the private sector and state/local agencies, to reduce redundant activities and leverage investments wherever possible. To this end, DHS led a government-wide effort, in partnership with the private sector, to build an interoperable framework for credentialing across the spectrum. This framework allows for credentials to be reused—by establishing common rules for levels of trust and uses associated with each type of credential, interoperability across populations, common processes for physical and logical access control systems. This effort is directly in line with the policy established through the DHS Credentialing Framework Initiative (CFI). The CFI established several guiding principles—including "enroll once, use many" for information reuse for individuals applying for multiple DHS privileges and associated credentials and vetting, associated with like uses and like risks, should be the same. The CFI provides a cohesive framework, with consideration for privacy, security risks, mission requirements, information sharing and other capabilities incorporated to ensure common strategies and objectives across DHS programs.

TSA has worked hard to align programs' security threat assessments by establishing the same eligibility requirements, offering a standard waiver and appeal process, and leveraging the same fingerprint-based criminal history records check to reduce redundancy and costs for workers. For example, the Transportation Worker Identification Credential (TWIC) program is able to offer TWIC applicants a reduced cost, from $132.50 to $105.25, when the applicant already has received a comparable security threat assessment, such as:

- Hazardous Materials Endorsement (HME).
- Merchant Mariner Credential/Document administered by the United States Coast Guard.
- Free and Secure Trade (FAST) card administered by United States Customs and Border Protection.

Another example is that the Air Cargo worker requirements for a security threat assessment accepts as comparable a valid Commercial Drivers License (CDL) with HME, TWIC, and FAST, as well background checks associated with Security Identification Display Area (SIDA) badges.

Question 4. There are approximately 150,000 miles of freight railroad tracks in the United States, on which many commodities, crucial to our Nation's economy, are carried. Maintaining the security of our Nation's railroad system, by monitoring the transport of security sensitive materials, or mitigating threats of terrorist attacks, is an important area for DHS and TSA to address. The 9/11 Act required DHS to develop a National Strategy for Railroad Transportation Security and submit a report to Congress by August 2008, detailing security assessments and the cost to implement the strategy. When will this report be submitted and will you commit to focusing the Department's efforts on our Nation's surface transportation security?

Answer. The Transportation Security Administration's (TSA) report entitled the "Railroad Transportation Security Risk Assessment and National Strategy" in response to the requirements in section 1511 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) is in the final stages of review at TSA. The Railroad Security Risk Assessment (RSRA) will describe the strategic level risks to the freight rail mode. TSA will provide context for rail risk in the transportation sector in the Transportation System Security Risk Assessment (TSSRA), which is a comprehensive national risk assessment that is required by both the Fiscal Year 2009 and Fiscal Year 2010 Appropriations language. Both reports are nearing completion.

The RSRA will also include a National Strategy for Railroad Security. This strategy has been synchronized with the upcoming update of the Rail Annex to the Transportation System Sector Security Plan (TSSSP), as part of the National Infrastructure Protection Plan required by Homeland Security Presidential Directive 7. In order to streamline and coordinate strategic planning, it is intended that the updated TSSSP Rail Annex will supersede the RSRA report's rail strategy. Both strategic planning documents will reflect the currently assessed risk in the rail system and the larger transportation system.

DHS also employs a variety of programs and policies that are focused on ensuring the security of the Nation's railroad transportation system. On November 26, 2008, TSA issued a final rule (73 FR 72130) for rail transportation security. The rule requires freight and passenger rail carriers, as well as shippers and certain receivers of rail security-sensitive materials (RSSM), to appoint a primary, and at least one alternate, rail security coordinator to serve as TSA's main point of contact, available on a 24/7 basis, to receive intelligence information and coordinate security-related activities. These covered entities are also required to report significant security concerns to TSA. Freight railroad carriers, as well as certain rail hazardous materials shippers and receivers, are also subject to the chain of custody provisions (49 C.F.R. 1580.107), which requires a positive and secure transfer of custody of a rail car containing RSSM at points of origin, delivery, and interchange, and includes certain requirements for physical security inspections of RSSM rail cars. Pursuant to the 9/11 Act, TSA is required to issue a regulation that would require an employee security training program for surface modes of transportation. Under the 9/11 Act, the rules cover freight railroad carriers, as well as public transportation agencies (including rail mass transit and bus systems), passenger railroad carriers, over-the-road bus operators, and certain motor carriers)."] The rules would establish propose minimum elements for the training programs addressing security awareness, terrorist behavior recognition, and threat and incident prevent and response for front-line employees. As also required by the 9/11 Act, TSA is developing regulations for railroad carriers to conduct vulnerability assessments and develop security plans.

TSA, in conjunction with the private sector, has also developed a list of 24 Security Action Items (SAIs). Distributed in June 2006, these security guidelines identified best practices, which freight railroads and their employees should implement to reduce the risk associated with the transportation of toxic inhalation hazard (TIH) materials. TSA also conducts Rail Corridor Assessments (RCAs), which focus on assessing the vulnerabilities of high-population areas where TIH materials are moved by rail in significant quantities. The RCAs provide site-specific mitigation strategies and lessons learned, and supported the development of the SAIs. These vulnerability assessments have also led to the implementation of a TIH Risk Reduction Project. Implemented in 2007, the Project focuses on objectively measuring the risk reduction associated with the rail transportation of TIH materials through 46 High Threat Urban Areas. As of October 2009, the objectively-measured risk has been reduced 80 percent as compared to the base measurement year (2006). The agency will continue to measure the ongoing risk associated with the movement of TIH shipments by rail, with the goal of a 10 percent risk reduction over the previous year.

Comprehensive Reviews conducted by TSA also provide a thorough evaluation of the security of a specific rail corridor and a comparative analysis of risk across transportation modes and critical infrastructure sectors in a specific geographic

area. Additionally, TSA's Corporate Security Review program, an "instructive" review of a company's security plan and procedures, provides the government with a general understanding of each company's ability to protect its critical assets and its methods for protecting hazardous materials under its control. The Intermodal Security Training and Exercise Program (I–STEP) is also being utilized by TSA to enhance the preparedness of the Nation's surface transportation network. I–STEP has been used by the TSA Freight Rail Security Division to facilitate discussions regarding the information-sharing processes and coordination between the Federal Government and the freight rail industry, particularly during heightened states of alert.

The TSA Freight Rail Security Division has also developed a critical infrastructure risk assessment tool for freight rail bridges. This tool is designed to measure the criticality and vulnerability of freight rail bridges in the United States, and will serve as the factual and analytical baseline to develop and propose security enhancements and mitigation strategies for critical railroad infrastructure. In Washington, D.C., DHS has also funded the National Capital Region Rail Security Pilot project to demonstrate the effectiveness of a suite of intrusion detection technologies in a freight railroad environment, specifically the D.C. Rail Security Corridor (DCRSC). The DCRSC is a seven-mile long corridor extending from the Anacostia River across the Potomac River. This pilot project included numerous components, including a virtual security fence that will detect moving objects, perimeter breaches, left objects, removed objects, and loitering activity. Data from the fence and the gates will be encrypted and transmitted simultaneously to multiple locations, such as the U.S. Capitol Police, U.S. Secret Service, other applicable Federal or local agencies, and CSX Transportation. Additionally, TSA is initiating a pilot project in FY 2010 to test security technologies on critical railroad bridges and tunnels.

The DHS National Protection and Programs Directorate—Office of Infrastructure Protection has also engaged the Rail Subsector in activities, projects, and initiatives, including conducting 55 Enhanced Critical Infrastructure Protection Initiative visits, 10 Computer-Based Assessment Tool visits, 39 Site Assistance Visits, 121 Buffer Zone Plans, and provided $15,171,500 in Buffer Zone Protection Program grant funding to local law enforcement to increase preparedness capabilities in communities surrounding high priority Rail Subsector infrastructure. The TSA Freight Rail Security Grant Program also makes funds available for security training of frontline employees, the completion of vulnerability assessments, the development of security plans within the freight rail industry, and the installation of tracking systems for railroad cars containing TIH.

Question 5. Earlier this year, the House passed a TSA Reauthorization bill. This Committee will likely work on a TSA Reauthorization proposal sometime in the coming year. Does DHS/TSA intend to submit a formal reauthorization proposal for the Committee to consider?

Answer. The Department of Homeland Security is reviewing a number of legislative proposals that may be appropriate for consideration in a Transportation Security Administration (TSA) authorization bill and looks forward to assisting the Committee in promoting a package of proposals that advance security in all modes of transportation. Among other things, the legislative proposals considered by the Committee in 2010 should consider the need for implementing new technologies in aviation security and ensuring that individuals who present a threat to our Nation's security are not permitted to board overseas flights to the U.S. Additionally, I hope the Committee would act upon the legislative proposal forwarded to the congressional leadership in May 2009 to authorize the Transportation Security Administration to incrementally adjust the aviation passenger security fee to cover a larger share of the cost of aviation security. I look forward to working with the Committee on any authorization language they will be introducing during the Second Session of the 111th Congress.

Question 6. It has come to my attention that only a small percentage of the Port Security Grant funding from Fiscal Years 2007, 2008, and 2009 have made it to the facilities that have been awarded grants. Can you explain where the delay has been in distributing these funds, and what steps are in place to ensure timely distribution? What percentage of the grant funding has actually made it to the recipients?

Answer. Since Fiscal Year (FY) 2007, the Department of Homeland Security (DHS) has awarded over $1.2 billion in Port Security Grant Program (PSGP) funding. Of this amount, approximately $49 million has been drawn down by recipients through FEMA's electronic Payment and Reporting System (PARS). This equates to approximately 4.1 percent of the total awarded funds drawn down by recipients. Although this is a relatively low percentage, drawdown figures should not solely be used to gauge program progress or lack thereof.

Each PSGP award has several special conditions that must be formally accepted by the recipient, some of which place holds on funds until met. The two special conditions that most significantly impact releasing funds and drawdown rates are the requirements for budget reviews and Environmental and Historic Preservation (EHP) reviews. These reviews take time and can vary by grant based on dollar amount, complexity of projects, grantee responsiveness, department priorities, workload, and staffing.

In FY 2007 and FY 2009, the PSGP received additional appropriations, essentially making two rounds of grants for these years. In addition, beginning with the FY 2007 Supplemental round, the highest risk port areas were required to assign a "Fiduciary Agent" (FA), who serves as FEMA's grantee and point of contact for all grant matters. The FA works at the local level with the Captain of the Port (USCG) to foster regional collaboration and prioritize projects for submission to FEMA. A series of deliverables are required to be submitted to FEMA and must be approved prior to submitting projects. These include a Concept of Operations (CONOPS) document and a Port-Wide Risk Management Plan (PWRMP). These deliverables can take 12–18 months to complete and grant funds may be used in their development.

Once these deliverables are submitted and approved by FEMA, the FA submits projects for review and approval. Even before FEMA receives the projects, they are reviewed and prioritized at the field level by the local Captain of the Port. Because each FA is on a different timetable, FEMA continually receives projects for review and must convene review panels of subject matter experts from across DHS. These panels take all of our grants staff away from their regular duties for many hours to review projects. If projects are not approved, they must be sent back to the FA for resubmission, causing further delay. Once projects are approved, they are submitted for budget and EHP clearance to release funds.

Once FEMA releases funds (either partial by project or the entire award), the recipient is notified and may drawdown against the grant through PARS. Of the $1.2 billion in PSGP funding awarded from FY 2007 to present, $223.5 million or 18.1 percent of total funding has been released to grantees. FEMA does not control or dictate when recipients must drawdown funds. Each recipient follows their local protocols. Funds may be drawn down anytime during the award period and up to 90 days following the end of the award period.

FEMA routinely engages with port stakeholders to listen to concerns and suggestions for improving the program. This past fall, FEMA invited all of the PSGP FAs to Washington, D.C. for a two-day workshop on how to improve the efficiency of the program.

One significant change with the FY 2010 PSGP is that all FA projects are due to FEMA 45 days after application close date. All projects will be reviewed at one time by one panel of subject matter experts. This will put all FAs on the same timetable and will eliminate the current practice of reviewing projects on a rolling basis and expedite the release of funds.

For existing awards (FY 2009 ARRA and prior), FEMA has made significant strides in releasing PSGP funding. Thanks to dedicated contract support personnel, the EHP backlog has been cleared. Additionally, it has been a priority of PSGP staff to review projects in a timely manner, release partial funds as projects are approved, and provide feedback to FAs as to status, particularly if projects are sent back requiring additional work. Finally, the majority of CONOPS and PRWMPs have been submitted and approved by FEMA, which now allows FEMA to concentrate on reviewing and approving projects.

FEMA continues to work to strengthen the PSGP, a complex program, with a multi-stage review process, co-managed with the subject matter expertise provided by the USCG.

Question 7. The Coast Guard uses a Marine Security Risk Analysis Model (MSRAM) to assess threats to critical infrastructure. However, the Department of Homeland Security still does not have one model of risk analysis that could be used by all agencies. Is there a plan to do so? Can we establish a quantifiable risk analysis tool for the Department that is adaptable for all DHS agencies?

Answer. The Department of Homeland Security (DHS) assesses homeland security risk by evaluating the potential for an unwanted outcome as a function of threats, vulnerabilities, and consequences associated with all hazards to the homeland. No single assessment of homeland security risks, such as the Marine Security Risk Analysis Model, will provide all the answers to the multitude of challenges the Department faces. As of now, there is no plan to develop one model or tool for risk analysis across DHS and other agencies. The goal of risk analysis is to inform decisionmaking, but since decisions at different agencies and within different sectors are unique, with different requirements, subject to different constraints, and based on

various degrees of information, it would be counter-productive to attempt to develop a single tool.

Homeland security risks are so complex and cross-cutting that our ability to manage risk effectively depends on our ability to integrate and manage a wide range of homeland security activities with Federal, State, local, tribal, territorial, and private-sector partners. A unified effort focused on integrated risk management concepts within the Department is essential to understanding and effectively managing homeland security risks.

Building and institutionalizing integrated risk management concepts and practices for homeland security takes time. DHS, however, has taken several critical first steps. The Department established the Office of Risk Management and Analysis (RMA) on April 1, 2007. RMA's mission is to enable and advance the effective management of risk by the homeland security enterprise. In April 2007, RMA created a departmental risk governance process by establishing the DHS Risk Steering Committee (RSC), which ensures collaboration, information sharing, and consensus building across the Department as we identify and integrate best practices for risk management and analysis. In September 2008, the RSC published a *DHS Risk Lexicon,* which establishes a common language for discussing risk-related concepts and techniques, and released an *Interim Integrated Risk Management Framework* in January 2009 that sets the foundation for a common approach to homeland security risk management.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. OLYMPIA J. SNOWE TO HON. JANET NAPOLITANO

Question 1. Madam Secretary, as you know, the Department has embarked upon an approximately 10M square feet headquarters consolidation at the St. Elizabeth's campus. How has the Department worked with the private sector to develop and implement an action plan?

Answer. The Department of Homeland Security (DHS) National Capital Region (NCR) Housing Master Plan was developed to provide the strategic vision for facilities that support a unified department, organizational structure, operations and culture. The plan outlines priorities of implementation and addresses the mission fragmentation caused by the Headquarters (HQ) elements being scattered in over 46 locations throughout the NCR. To meet the component office space requirements through FY 2011 for headquarters facilities, the Department will require about 8 million gross square feet (GSF) of office space in the NCR with the potential to grow to 10 million GSF by FY2015.

While St. Elizabeths will accommodate the main Department and Component HQ mission execution functions with 4.5 million GSF of office space, it does not have the capacity to accommodate all of the DHS mission support elements. Therefore, the DHS NCR Housing Master Plan also proposes to consolidate the mission support elements that are currently dispersed throughout the NCR to support functional integration, improve effectiveness and efficient management of the real estate portfolio.

The end state real estate portfolio will include St. Elizabeths as the center of gravity for the Department Headquarters and federally owned locations at the Nebraska Avenue Complex (NAC), the U.S. Secret Service HQ and the DHS space at the Ronald Reagan Building. DHS has two long-term leases that will also be retained—the TSA location in Arlington, VA and the ICE space in SW Washington, D.C. A Mission Support Consolidation Prospectus for lease authority was submitted by General Services Administration (GSA) to Congress on October 18, 2009 to acquire a 1.2 million Rentable Square Feet (RSF) lease to consolidate the remaining locations.

The Department and GSA have coordinated with the private sector throughout the past four and a half years. We've received many capabilities briefs from private sector entities with an interest in the headquarters consolidation initiative including both the St. Elizabeths Campus and the Mission Support Consolidation initiatives.

GSA also engaged the market in development of the mission support lease prospectus to verify DHS requirements could be achieved while ensuring competition among the private sector offerors.

On October 26, 2009, GSA and DHS sponsored an Industry Day at the Ronald Reagan Building to inform the business community on upcoming opportunities that will be available with the St. Elizabeths development. Approximately 1000 people attended the forum which provided opportunities for networking, sessions on DHS and GSA Small Business goals and practices. In addition, the GSA Federal Acquisition Service held a pre-solicitation conference in Washington, D.C., on December 14,

2009, for the St. Elizabeths Campus Technology Integration Program (TIP). The GSA acquisition strategy for the TIP is to provide an Information Technology (IT) contractor to supply materials and installation services for an enterprise wide IT campus infrastructure.

Question 2. How does the Department intend to facilitate interaction across all DHS sites in the region through this consolidation?

Answer. The establishment of St. Elizabeths as the Consolidated DHS HQ with all component leadership/mission execution functions represented and collocation of Component Operations Centers with the NOC, will form the foundation for building a department that is culturally, operationally and administratively unified. The campus structure optimizes our prevention and response capabilities though enhanced communication, coordination and cooperation and promotes interaction through shared use of common support and administrative facilities. The Technology Integration Program (TIP) being developed for St. Elizabeths is also being designed to consider the overall headquarters consolidation initiative and provides an enterprise wide IT infrastructure to promote and enhance communications across the consolidation sites. In addition, lessons learned with the St. Elizabeths development will be leveraged across the entire consolidation effort.

Execution of the St. Elizabeths development without addressing the rest of the mission support functions will continue to impact the effective communications, coordination and cooperation among the headquarters and components due to the increasingly scattered nature of the portfolio.

Question 3. As you may know, Saint Elizabeths could become a security technology corridor that advances the mission of Department of Homeland Security while simultaneously driving innovation and private sector commercialization. How does the DHS intend to advance the Department's mission while driving innovation and private sector commercialization at the Saint Elizabeths campus?

Answer. The Department and GSA are closely coordinating with the District of Columbia, the National Capital Planning Commission, the Council on Environmental Quality/Office of the Federal Environmental Executive, the White House Office of Urban Affairs and organizations such as the Chesapeake Crescent Initiative (CCI) to explore opportunities to promote sustainability and innovation in conjunction with the St. Elizabeths development (DHS and DC's efforts on the West and East Campus). There are also opportunities to link to broader community revitalization efforts with the Sustainable Communities and Neighborhood Revitalization initiatives.

The CCI is a regional collaborative effort formed by the Federal Government, the District of Columbia, and the state governments of Virginia and Maryland. CCI's goal is to focus on four areas: Regional Collaboration; Environment/Energy; Innovation/Economy; and Secure and Sustainable Development. CCI established the St. Elizabeths/Security Working Group to address three specific objectives: (1) Convening stakeholders—Federal, State and City governments, the private sector, nonprofit organizations, universities across the region, DHS employees and the community of citizens in Ward 8; (2) Communicating progress and identifying challenges that require collaboration to achieve success—through meetings, events and academic research support; and (3) Serving as a catalyst for action—to set new environmental standards with renewed historic resources, improve transportation, build new commercial and residential communities, foster education and workforce development and identify and deploy innovative solutions to advance our Nation's security capability—all in support of a new home for DHS, a revitalized community and a stronger regional economy with 21st Century jobs. The Department supports this effort with participation by our Headquarters Consolidation Program Office and the Chief Commercialization officer. Along with GSA, we will continue to work with CCI and our District partners as they transform their approved high level East Campus Redevelopment Framework Plan into specific development initiatives.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHN ENSIGN TO HON. JANET NAPOLITANO

Question. Following the release of the TSA screening document entitled "Screening Management Standard Operating Procedures" dated May 28, 2008, that was placed on a website and contained Sensitive Security Information including the identification cards of Members of Congress earlier this week, I submit the following questions:

How high up did the authorization have to go before the document was placed on the website?

Did the authorization go as high as the political appointees or was it just a career employee that placed the document online for all to read?

I understand that people were put on Administrative Leave following this release of TSA security sensitive information. Were the people who authorized the release of this information also put on Administrative Leave?

I understand that there are currently 2 simultaneous investigations ongoing with regard to the release of this information, an Inspector General review and an Office of Investigations review. How long will it take to complete the review process? Can you provide a timeline as to when people can be held accountable for this release? When policies may be changed?

Answer. After conducting an Executive Leadership conference call on the night of December 6, 2009, the Transportation Security Administration (TSA) Acting Administrator implemented a number of actions to address the breach of Sensitive Security Information (SSI), including a directive to the TSA Office of Investigations (OI) to investigate the cause and circumstances of the breach of SSI. The OI began to investigate the matter until TSA was notified that the Department of Homeland Security Office of the Inspector General (OIG) would be investigating the same matter at my direction. As required by a DHS Management Directive, OI suspended its investigation and deferred the matter to OIG. Because these questions are the subject of the OIG investigation, I am not able to provide specific responses until the OIG completes its investigation and issues a final report.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JIM DEMINT TO HON. JANET NAPOLITANO

Question 1. When will you repeal the current prohibition on collective bargaining at TSA (ADM Loy Memorandum of January 8, 2003 Subject: Determination Regarding Collective Bargaining TSA Security Screeners)?

Secretary Napolitano I was disappointed to hear this morning that you had decided to agree to a collective bargaining agreement with the TSA Screeners, overturning a policy which has kept the traveling public safe for close to 7 years. At the hearing you stated, there are examples around the country of collective bargain agreements with law enforcement agencies that have similar responsibilities where you have carve-outs in effect, in the collective bargaining context to make sure those types of things are not part of the collective bargaining agreement. We would anticipate in this context with the TSOs that we will be able to reach such an understanding. Please provide a detailed plan outlining the carve-outs you will insist upon in a collective bargaining agreement including a rationale for the carve outs. Are there any workers who you believe should not be allowed to be included in a collective bargaining agreement?

Answer. As I stated in my testimony, I am waiting for the confirmation of a nominee to head the Transportation Security Administration (TSA). I expect any future nominee to make a thorough review of the matter, including the alignment of any decision about collective bargaining with our profound commitment to maintain and continue to improve transportation security, before presenting recommendations to me on collective bargaining at TSA.

With regard to which positions might be included in a bargaining unit of Transportation Security Officers afforded collective bargaining rights, although no decision has been made, I would expect that such a unit determination would follow prevailing law covering Federal employees which excludes those employees deemed to be supervisory or confidential employees.

Question 2. At the hearing you stated, "I will give you an example, even without a collective bargaining agreement right now, our TSA employees have been very eager to, whenever we've had an emergency and we need to, for example bring more people down to help staff an airport in a hurricane, when the people who have to work there have to stay home and work with their families because their houses have been destroyed or whatever. We have never had a problem, in my experience, with employees being willing to move to a place where a crisis is occurring."

Will you insist that as a condition of repealing the collective bargaining agreement prohibition that any collective bargaining agreement empower the Administrator of the TSA to have the authority to transfer and reassign personnel in response to security threats for the duration of the threat without first getting the approval of their union?

Answer. As stated, I am awaiting the confirmation of a nominee to head the Transportation Security Administration (TSA). It is my expectation that any future nominee will conduct a thorough review of all matters concerning collective bargaining at TSA prior to making recommendations to me. I will ensure that any deci-

sion that is made takes full account of security concerns, and enables TSA to continue to maintain and improve transportation security on a daily basis.

Question 3. Madam Secretary, for several years your department has been trying to address ways to better coordinate or harmonize credentialing and background check processes. Today, for example, we know that truck drivers can undergo up to four separate costly background checks* through agencies within your department to perform their job duties. Are you aware of this issue? If so, please tell us what DHS is doing to coordinate or consolidate these multiple screening and credentialing processes.

Answer. It is DHS's goal, in partnership with the private sector and state/local agencies, to reduce redundant activities and leverage investments wherever possible. To this end, DHS led a government-wide effort, in partnership with the private sector, to build an interoperable framework for credentialing across the spectrum. This framework allows for credentials to be reused—by establishing common rules for levels of trust and uses associated with each type of credential, interoperability across populations, common processes for physical and logical access control systems. This effort is directly in line with the policy established through the DHS Credentialing Framework Initiative (CFI). The CFI established several guiding principles—including "enroll once, use many" for information reuse for individuals applying for multiple DHS privileges and associated credentials and vetting, associated with like uses and like risks, should be the same. The CFI provides a cohesive framework, with consideration for privacy, security risks, mission requirements, information sharing and other capabilities incorporated to ensure common strategies and objectives across DHS programs.

DHS has begun efforts on a number of initiatives to implement this streamlined process and reuse of vetting results:

- *Reusing Assessments Conducted.* TSA is working hard to align the programs' security threat assessments (STAs) by establishing similar eligibility requirements; offering a standard waiver and appeal process; and leveraging the same fingerprint-based criminal history records check to reduce redundancy and costs for workers. There are several examples of where this is apparent today:
  - The Transportation Worker Identification Credential (TWIC) program is able to offer TWIC applicants a reduced cost, from $132.50 to $105.25, when the applicant already is receiving a comparable security threat assessment, such as one for:
    - —Hazardous Materials Endorsement (HME).
    - —Merchant Mariner Credential/Document administered by the United States Coast Guard.
    - —Free and Secure Trade (FAST) card administered by United States Customs and Border Protection.
  - Another example is that the Air Cargo worker requirements for a security threat assessment accepts as comparable a valid Commercial Drivers License (CDL) with HME, TWIC, and FAST, as well background checks associated with Security Identification Display Area (SIDA) badges.
- *Establishing ability to electronically verify person's license, status, or privilege.* In order to issue fewer documents and reuse existing cards, the various organizations interacting with these populations must be able to electronically authenticate the credential presented and that the person is authorized access.
  - For example, in order for DHS to stop issuing separate HME endorsements to the holder of a TWIC, law enforcement must have the ability to electronically validate that TWIC, an ability they do not currently have.
- *TSA TTAC Modernization.* The TSA modernization effort, an initiative to enhance TSA vetting and credentialing programs that affect the security of all critical transportation sectors, will play a critical role in achieving these goals. TSA is modernizing its business processes and systems to improve and maintain the effectiveness and efficiency of transportation security threat assessments.

Question 4. As I'm sure you are aware, my amendment requiring the completion of 700 miles of reinforced double-layer fencing along the U.S. Southern border by

* DHS Background checks: Hazardous Materials Endorsement (HME), Transportation Worker Identification Credential (TWIC), Free and Secure Trade (FAST) program and Air Cargo Security Threat Assessment.

the end of next year was stripped from the Department of Homeland Security Appropriations bill just a few weeks ago. How do you propose we move forward and solve the border security problems our Nation is currently facing without completing this fence and giving the law we passed a chance to work?

Answer. First and foremost, all efforts aimed at addressing threats to U.S. border security must occur within an institutionalized concept of operations that consistently leverages the proper, integrated mix of Department of Homeland Security (DHS), other Federal, State, tribal and local resources to gain effective control, or situational awareness, where applicable, in prioritized areas of greatest threat, vulnerability and risk. As a stakeholder, CBP Office of Border Patrol continues to implement the following:

- Focusing on the capability to rapidly deploy personnel/resources to areas deemed highest risk through intelligence and predictive analyses along the Southern and Northern borders.
  - For example, state-of-the-art enforcement technology, such as Mobile Surveillance System vehicle(s).
- Expanding partnerships with other Federal, state, tribal and local agencies to develop, refine and institutionalize a nationwide collaborative, cooperative enforcement approach such as the Alliance to Combat Transnational Threats (ACTT).
  - Combines capabilities and resources of Federal, state, tribal and local law enforcement agencies to deny, degrade, disrupt and dismantle criminal organizations.
  - Leveraging participation in fusion centers to institutionalize intelligence-driven operations.

Question 5. Related to border security, one of the greatest threats currently facing our Nation and our Southern border in particular is the presence of violence and illegal drug trafficking taking place between the U.S. and Mexico. Back in March, you announced a "Comprehensive Response" border security policy that:

Invested $700 million this year under the Merida initiative to work with Mexico on law enforcement and judicial capacity,

Increased DOJ, DHS, and Treasury personnel and efforts directed at the Southwest border, and

Renewed the U.S.' commitment to stemming the demand for illegal drugs here at home.

Now that we are approaching the end of the year, can you provide for us a brief update on the implementation of this plan, and describe what impact this money and these efforts have had on the present situation along the southern border?

Answer. The Department of State (DOS) is the overall U.S. Government (USG) lead for Merida Initiative activities including the acquisition of all technology equipment and software, such as Non-Intrusive Inspections Equipment (NIIE). DOS also coordinates and obtains all licenses or permits associated with the acquisition, transportation, delivery and or shipment of equipment and software to be donated to the receiving governments. CBP has established an inter-office Merida Committee to coordinate with DOS, DHS and others and to steer CBP implementation actions.

- CBP and DOS established an Inter-Agency Agreement (IAA) to fund a CBP Advisor to the Narcotics Affairs Section (NAS) of the State Department at the U.S. Embassy in Mexico responsible for providing technical assistance and expertise related to purchases under the Merida Initiative in Mexico. The advisor is now working in this capacity.
- CBP developed an IAA with DOS to provide training and technical support for Merida Initiative activities. This IAA was awarded on September 30, 2009. Specifically, this IAA provides for the training of 44 dogs for Mexico Customs, scheduled to occur in 2010. The training consists of 3 classes, each 11 weeks long. The program includes the curriculum for train-the-trainer as well. The first class will begin January 18, 2010. The IAA also provides for the training of 50 SSP Officers on five ZVB X-ray vans (vans already purchased by NAS) which will occur via five, ten-student classes held in or around Mexico City. CBP will continue to work with Mexico Customs on their curriculum to assist in moving from a revenue-based to a law enforcement-based agency. Additionally, CBP conducted an assessment of Mexico Customs basic academy training. The resulting gap analysis will be a road map to guide Mexico Customs in changing their curriculum from revenue-based to law-enforcement based.

CBP will continue discussions of the way forward on geographical expansion of the Operation Against Smugglers Initiative on Safety and Security (OASISS) program. OASISS is a binational prosecutorial program focused on combating human smuggling across the Southwest Border by identifying and prosecuting Mexican nationals arrested for alien smuggling in the U.S. A memorandum of understanding for information sharing with Mexico is being reviewed by the Office of Border Patrol.

CBP, in coordination with DHS, has partnered with Department of Defense (DoD) Joint Task Force North, and other border security entities in the U.S. and Mexico to develop a plan to gain greater control over the Arizona Border. The plan is called the Operational Alliance to Combat Transnational Threats (ACTT), though originally designated the Arizona Operational Plan (AOP). A key component of the plan is to operate collaboratively with the Mexican SSP Federal Police to obtain greater operational control of the Arizona/Sonora border. A Declaration of Cooperation with the SSP has been drafted for the purpose of illiciting a sustained commitment of resources from the Government of Mexico to control the Arizona/Sonora border. The Declaration institutionalizes lessons learned from the ACTT bilateral cooperation efforts and expands these collaborative efforts along the entire Southwest border, closing smuggling corridors that impact upon both countries' national security.

Question 6. As part of any collective bargaining agreement, will you require that the agreement allow any TSOs to withhold the portion of their union dues that finances lobbying and political activity?

Answer. Unlike the private sector, employees in the Federal Government are not required to pay union dues or agency fees, even when there is a collective bargaining agreement in effect. Accordingly, there would be no reason to include such a provision in a collective bargaining agreement at the Transportation Security Administration (TSA).

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ROGER F. WICKER TO HON. JANET NAPOLITANO

Question 1. I understand the Department has unmanned aerial system (UAS) assets through Customs and Border Protection (CBP). Opportunities for use of these systems could expand in the future to other components of DHS and assist the Department in carrying out its significant mission. The Air Force has acknowledged the difficulty of coordinating with the Federal Aviation Administration (FAA) regarding the operation of DOD-related UAS assets in domestic airspace. It is important that we ensure a strong partnership between your Department and the FAA on similar efforts. Please explain the process between DHS and FAA to utilize domestic airspace for the UAS activities.

Answer. Currently, CBP Office of Air and Marine submits, through an online process, an application for a Certificate of Authorization (COA). COAs are required due to current Federal Aviation Regulations (FARs) written only for manned aircraft and that no UAS standards have been developed and codified through rulemaking.

The COA application is very in-depth and contains detailed information concerning the UAS aircraft operating location and altitudes; supporting equipment and systems. The application also solicits information on personnel and pilot qualifications. Last, the application requires aircraft airworthiness information; potential impact to other airborne aircraft; people and property on the ground; communication requirements; and emergency aircraft procedures. Risk mitigation is a paramount factor.

If the COA application is approved allowing the CBP UAS to operate in the National Airspace System (NAS), it is disseminated to CBP and to the FAA facilities whose airspace the UAS will operate within. FAA facility air traffic controllers are trained on the operational capabilities and limitations of the UAS as well as the restrictions and operational parameters within which the UAS must operate. Continuing coordination and collaboration exists to amend, if necessary, a provision contained within the COA. COAs are currently issued by the FAA from a one-time authorization to standing authorizations, but not to exceed one calendar year. Standing authorizations can be renewed after undergoing the same scrutiny as an original application. Though there are various sizes of UASs in use, CBP operates the second largest UAS in service today—the MQ–9 Predator B. At 10,000 lbs and with a wingspan of 66 feet, it is the size of a large general aviation aircraft and is flown by CBP and USCG personnel, all with FAA pilot licenses. The pilots of the UAS communicate with and receive air traffic control instructions from FAA controllers exactly as any aircraft would be controlled and operate within the NAS.

Question 2. Must DHS work with any other Federal entities to fully utilize the Departments UAS assets?

Answer. Yes, first and foremost with the Federal Aviation Administration (FAA) for permission to fly in the National Air Space through the Certificate of Authorization process. Though CBP operates the MQ–9 Predator B, it is a DHS and national asset. CBP is continuously partnering within DHS and other government agencies in an attempt to demonstrate the capabilities this asset provides for law enforcement, incident management, search and rescue, DoD support, etc. No manned aircraft in the U.S. Government inventory provides the persistent and sustained surveillance that the Predator is capable of.

Question 3. How can the relationship between DHS and FAA regarding the use of UAS in domestic airspace improve?

Answer. Language in Section 1036 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110–417) called for a more cooperative relationship between DoD and the FAA in obtaining access to the NAS with UASs and as such the establishment of a joint Executive Committee (EXCOM) to resolve conflicts and disputes. Recognizing that DHS has a major role and requirement in obtaining access to the NAS, DHS was invited to participate in the EXCOM. DHS, DoD, NASA, and FAA are currently cooperating and collaborating on a process to safely, efficiently, and timely gain increased and routine access to the NAS.

Question 4. Are you aware of any instances where the Department was delayed in utilizing UAS assets as a result of interagency coordination?

Answer. Ad-hoc, non-routine access to the NAS by CBP UASs have been processed by the FAA in an expeditious manner and ultimately never denied. CBP operates under one of four types of COAs; mission (operational), training (pilots), emergency, and disaster (FEMA or Federal or State support).

Through the EXCOM, shortfalls have already been identified within the COA application process. Corrective actions have been recommended by a COA interagency working group which address FAA resource issues, reduced COA processing timelines, standardized application information, etc. If implemented, perceived delays should be minimized and COA processing burdens on the FAA and proponents will be greatly reduced.

Question 5. Congress recently passed the Consolidated Appropriations Act of 2010, which was subsequently signed into law by the President on December 16, 2009. The law includes a mandate that Amtrak consult with the Transportation Security Administration (TSA) on developing and implementing guidance and procedures to provide for checked firearms on Amtrak routes that permit checked baggage. The law also requires for consultation with TSA in reporting to Congress on these efforts within 180 days of enactment.

Amtrak's consultation with the TSA is not only mandated, but it is vital to the successful implementation of this important program. What steps will you pursue to ensure timely and effective consultation with Amtrak on these directives?

Answer. In accordance with section 159 of the Consolidated Appropriations Act, 2010 (Pub. L. 111–117), the Transportation Security Administration (TSA) has initiated consultation with Amtrak to develop and implement guidance and procedures to provide for checked firearms on Amtrak routes that permit checked baggage. Consistent with the statutory mandate, Amtrak and TSA will continue to consult thoroughly on security matters implicated by the requirement to develop and implement a program for transport of firearms and ammunition in checked baggage. Amtrak and TSA have agreed to form a joint working group for this purpose.

Question 6. The President's budget request for Fiscal Year 2010 included $856 million for Explosives Detection Systems (EDS), which is a needed increase from the previous enacted level in Fiscal Year 2009 of $294 million. Even with the increase for EDS that was recently passed by Congress, the need of airports across the country to recapitalize checked baggage screening equipment and accelerate the deployment of in-line systems remains of the upmost importance. Without continued funding it will be impossible to provide the latest, cutting-edge technology necessary to keep the aviation sector secure from the threats of terrorism.

As you know, many of these checked baggage screening systems that were deployed immediately after September 11, 2001 have reached the end of their life cycles and the costs to keep these older technology systems functioning with minimal down time is becoming prohibitive.

Will you support maintaining the Fiscal Year 2010 EDS procurement and installation funding levels at our Nation's airports in Fiscal Year 2011 necessary to maintain the Electronic Baggage Screening Program (EBSP)? With the threat of new explosives evolving rapidly how do you see this factoring into the replacement of older

equipment such as Explosive Trace Detection (ETD) with newer equipment that is equipped to change with these continued new threats?

Answer. The funding level for Fiscal Year 2011 will be released in the President's budget in February. The threat of new explosives and new threats to aviation security continues to evolve. The Transportation Security Administration (TSA) has developed a Strategic Plan for the Electronic Baggage Screening Program, which includes a central goal of replacing Explosive Trace Detection (ETD) equipment used for primary screening with Explosives Detection Systems (EDS) machines at airports. There is currently an on-going effort to replace primary-screening ETD machines with Reduced-Size Explosive Detection System (RSEDS) at Category X–III airports. In Fiscal Year 2010, from January to September, TSA plans to deploy on average 20–25 RSEDS units per month to airports nationwide. RSEDS provides a less intensive manpower approach, plus the increased screening capabilities of EDS relative to ETD equipment for primary screening. Please note that ETD equipment will continue to play a critical role in assisting Transportation Security Officers in resolving suspect baggage that have alarmed the EDS equipment (referred to as secondary screening).

Among the actions being taken to address evolving new threats, TSA is taking steps to pursue a full and open competitive procurement for reduced-size, medium-speed, and high-speed EDS technologies. This procurement will segment the technologies into distinct system types, provide for increased competition, enhance detection and operational capabilities, and provide for a reduced total cost of ownership.

Question 7. Continued efforts by the Transportation Security Administration to enhance security at our Nation's airports remain vital to our Nation's security. The Administration's focus on the top 20 to 25 airports to enhance security for 95 percent of passengers in the United States is not reflective of the true situation since a significant majority of passengers begin their trips at medium and small airports. According to figures from the Department of Transportation's Bureau of Transportation Statistics, 54 percent of the passengers begin their trips at the Nation's top 25 airports, while 46 percent of the passengers begin their air travel at the next 225 airports. Since checked baggage is screened at originating airports, medium and small airports cannot be neglected if aviation security is truly to be enhanced. In knowing that two of the highjackers on 9/11 began their flight at a small airport in Bangor, Maine, what steps are you taking to ensure that the need for medium and small airports to receive the latest explosives detection systems is as important as the Category X airports?

Answer. The needs of small and medium airports are taken into consideration by the Transportation Security Administration (TSA) to enhance security at our Nation's airports. The Fiscal Year (FY) 2009 budget included $87 million for medium- and small-sized airports for the procurement and deployment of certified Explosive Detection Systems. The FY 2010 budget includes an additional $218 million for the needs of medium- and small-sized airports. In addition, up to $50 million of the Aviation Security Capital Fund is used to make discretionary grants, including Other Transaction Agreements for airport security improvement projects with priority given to small and non-hub airports.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JOHNNY ISAKSON TO HON. JANET NAPOLITANO

Question. Will the Department of Homeland Security plan to launch the US–VISIT Exit program, and if so, will DHS plan to check departures on the Canadian and Mexican borders, as well as in seaports?

Answer. It should be noted that the Department of Homeland Security (DHS) currently has biographic exit information; however, the Department is currently weighing several options for adding biometrics based on pilots conducted over the past 6 years. The infrastructure at land borders does not easily lend itself to any consistent form of exit based on current technology.

Air/Sea

DHS has performed significant planning and testing over the past 3 years to examine possible solutions for integrating US–VISIT biometric exit requirements into the international air departure process. For more than 2 years, US–VISIT ran biometric exit pilots at 12 airports and two seaports. These pilots evaluated the use of both automated kiosks and mobile devices in port terminals. When the pilots ended in May 2007, an evaluation determined that the technology worked effectively but traveler compliance was low. DHS determined that biometric air exit needs to be integrated into the existing international traveler departure process.

On April 24, 2008, DHS published a notice of proposed rulemaking (NPRM) proposing that commercial air carriers and vessel carriers collect and transmit the biometric information of aliens to DHS within 24 hours of their departure from the United States. In the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act of 2009 (Public Law 110–329), Congress required DHS to test additional biometric collection before finalizing the Air-Sea Exit NPRM to ensure that the best available procedures are implemented.

From May 28 to July 2, 2009, US–VISIT tested biometric air exit procedures at two airports: Detroit Metropolitan Wayne County Airport and Hartsfield-Jackson Atlanta International Airport. In Detroit, DHS tested the collection of alien passengers' biometrics at the boarding gate by U.S. Customs and Border Protection officers. In Atlanta, DHS tested the collection of alien passengers' biometrics at Transportation Security Administration checkpoints. Consistent with Public Law 110–329, the Department has submitted an evaluation report of these pilots to the House and Senate Committees on Appropriations, as well as to the Government Accountability Office. The results of the pilot evaluation, combined with the review of public comments submitted in response to the NPRM, will inform the decision on the option to be selected for publication in the final rule.

Land

Biometrically recording the departures of aliens at U.S. land border ports of entry poses significantly greater challenges. Each year, our land border ports of entry see more than 300 million crossings at 170 port locations, including seasonal and other ports that are not open year round. Due to variations in infrastructure, environment, and traffic volume from port to port, a one-size-fits-all solution to acquiring biometrics from aliens crossing the border will be difficult. The Department is examining options for the land border environment that will not negatively impact the economy, the environment, or traveler safety.

Canadian and Mexican Borders

Seeking to maximize biometric information-sharing efforts in support of its exit program, US–VISIT took the lead in forming a Technical Working Group on Biometric Identity Management with the Canada Border Services Agency.

The working group has established joint biometric principles and is working on a framework to share biometric information related to third-country nationals entering Canada to establish exit from the United States. This work will progress over the next few years as Canada implements biometric capture capabilities for visa and port-of-entry operations. Canada plans to complete implementation of its biometric program by 2013.

Since Mexico is in the initial stages of developing its biometric capabilities for border and immigration control, there has not yet been an opportunity to share biometrics for exit purposes. US–VISIT continues to provide technical assistance in support of Mexico's efforts to incorporate biometrics into its immigration process under the Mérida Initiative.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAVID VITTER TO HON. JANET NAPOLITANO

Question 1. Please provide information on actions the Department is taking to ensure that ports that handle primarily oil and gas, not cargo, will remain secure.

Answer. The Coast Guard has a multi-tiered approach to ensuring the safety and security of ports which handle oil and gas.

The Coast Guard's Operation Neptune Shield identifies the Maritime Security and Response Operations (MSRO) activities which the Coast Guard Sectors will conduct and establishes their performance standards. The MSRO activities identified in this self-imposed operation are intended to deter, detect, prevent, protect against, interdict, and/or aid the recovery from attacks and include but are not limited to: waterborne, aerial, and shoreside patrols; security boardings; moving security zone enforcement (vessel escorts); and fixed security zone enforcement.

As mandated by the Maritime Transportation Security Act (MTSA), all oil and gas facilities and vessels calling upon them are required to maintain and implement approved security plans to ensure appropriate measure are taken to deter, prevent and respond to security threats and incidents. The Coast Guard verifies the adequacy of these security plans by conducting periodic plan review, compliance examinations and unannounced spot checks. As part of the mandated Area Maritime Security Committee (AMSC) process, strong partnerships have been formed with key stakeholders from state and local agencies and the maritime industry. These partnerships

have facilitated information sharing and a risk based approach to address maritime security.

The Coast Guard's International Port Security (IPS) Program, also required by the MTSA, assesses the effectiveness of anti-terrorism measures in foreign ports including those which primarily handle oil and gas. The IPS Program conducts visits to those ports to verify the adequacy of the security measures using the International Ship and Port Facility Security Code as the primary basis to determine if a country has effective anti-terrorism measures. The Coast Guard has visited the ports in approximately 150 countries which trade with the U.S. For those ports with inadequate security, the Coast Guard imposes "Conditions of Entry" on vessels arriving to the U.S. from them. These conditions of entry require these vessels to take additional security measures overseas or upon arrival to the U.S. to reduce the risk to U.S. ports.

The Coast Guard's Maritime Security Risk Analysis Model (MSRAM) is a terrorism risk analysis tool used to perform detailed risk analysis of the maritime transportation system and port critical infrastructure, including oil and gas facilities. MSRAM provides a means to use security assessments, consequence models, and threat information to numerically quantify risk across all ports and industry sectors. MSRAM identifies and prioritizes infrastructure based on defined terrorist attack scenarios, and informs the Coast Guard Captains of the Port (COTPs) and their Area Maritime Security Committees (AMSCs) on the highest risk critical infrastructure within their ports. Based upon this information, the COTPs and AMSCs have modified their Area Maritime Security Plans and prioritized Coast Guard and other law enforcement resources to protect the highest risk critical infrastructure in their ports.

Question 2. Many from Louisiana's maritime industries have voiced concerns about bureaucratic delays when their employees obtain TWIC cards. What is DHS doing to alleviate unnecessary delays while maintaining and improving security measures?

Answer. Since the national implementation of the Transportation Worker Identification Credential (TWIC) program, the Transportation Security Administration (TSA) has enrolled over 1.4 million workers associated with our Nation's maritime ports and vessels and issued credentials to those individuals who have been found eligible to receive a TWIC. With the rollout of any program of this size and complexity, there are always challenges to meet and process improvements to make. TSA is continually reviewing its enrollment, adjudication and credentialing issuance processes and procedures to improve efficiencies wherever possible and expedite the issuance of these credentials. An example of these efforts is our continual communications with stakeholders via the TWIC Stakeholder Communication Committee used to provide program updates and receive stakeholder input. Also, we have added new personnel and resources to facilitate the redress process for those individuals who have been deemed ineligible to hold a TWIC as a result of the security threat assessment. If there are any specific Louisiana Maritime Industry concerns, TSA would be more than happy to address them.

Question 3. While protecting vital American jobs, the Jones Act also serves to enhance maritime security. Please provide a status update regarding deliberations by CBP and DHS, underway since July, about whether to modify or withdraw several letter rulings concerning the transportation by foreign vessels of cargo to offshore energy sites.

Answer. Based on several substantive comments CBP received, both supporting and opposing the proposed action, and CBP's further research on the issue, CBP determined that the proposed modification and revocation of ruling letters relating to the Jones Act published in the Customs Bulletin on July 17, 2009, should be reconsidered. To that end, the proposal was withdrawn by a notice dated September 15, 2009, and published in the Custom Bulletin of October 1, 2009. Deliberations are still underway on this matter.

Question 4. My understanding is that CBP has been presented with at least two complaints of Jones Act violations occurring offshore in recent months. Please provide the Committee with an update on the status of those investigations. Also, please provide a full report at such time as any action is taken in those cases.

Answer. This case alleges that on two separate occasions certain merchandise was transported between Louisiana ports and locations on the Outer Continental Shelf by non-coastwise-qualified vessels.

In consideration of the potential penalty assessment in these allegations (at least $2 million for each case), it has been our recommendation that no penalty action be pursued until the specific facts of these alleged violations can be verified.

○