**The Honorable Janet Napolitano**

**Secretary**

**United States Department of Homeland Security**

**Testimony on**

**"Transportation Security Challenges Post 9-11"**

**Before the**

**United States Senate**

**Committee on Commerce, Science, and Transportation**

**Russell 253**
**December 2, 2009**
**10:00 a.m.**

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% 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% 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 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

[1] There are important differences between scanning and screening of maritime cargo, as defined by the SAFE Port Act. "Scanning" means utilizing nonintrusive 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.

the ground" at these ports. Importantly, these ports represent about 86% of all shipping into the United States.

*The 100% scanning issue*

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

---

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

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% 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 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 workforce, 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% 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

[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.

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 Supplemental 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% of air cargo is now undergoing screening. More than 95% 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% 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% 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 four years, TSA's highly trained Federal Air Marshals have flown millions of

[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.

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.

**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 timeframe 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 five 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% 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 workforce, 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 workforce.

**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.

[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.

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.

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