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

"EVALUATING PORT SECURITY: PROGRESS MADE AND CHALLENGES AHEAD"

JUNE 4, 2014

JOINT TESTIMONY OF

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

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

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

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

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

INTRODUCTION

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

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

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

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

OVERVIEW

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

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

RISK BASED AND LAYERED APPROACH

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

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

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

Understanding the Risk

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

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

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

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

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

Advanced Information and Targeting

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

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

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

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

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

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

Early Action Through Collaboration

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

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

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

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

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

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

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

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

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

Domestic Security Regimes

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

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

Also within U.S. ports, Coast Guard security regulations authorized by the SAFE Port Act and the Maritime Transportation Security Act (MTSA) require facilities, U.S. vessels, and designated foreign vessels calling on U.S. ports to conduct security assessments and to develop plans to address security vulnerabilities. The Transportation Worker Identification Credential (TWIC) is an important part of these efforts. The TWIC program ensures that workers needing routine,

unescorted access to secure areas of facilities and vessels are vetted against a specific list of terrorism associations and criminal convictions. The TWIC program is the first and largest federal program to issue a standard biometric credential for use in diverse commercial settings across the nation. The nationwide applicability and recognition of TWIC promotes an economically efficient and mobile workforce, building efficiency in normal conditions and resilience when port disruptions occur. TWIC holders, with a legitimate business case to do so, may enter and work on vessels and facilities throughout the country.

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

In addition, the Coast Guard conducts at least two security inspections annually at MTSA-regulated facilities, with one inspection being unannounced. This verifies that vessels and facilities in all Coast Guard Captain of the Port Zones are in compliance with TWIC requirements. In addition to the security activities taken by vessel and facility security officers, the Coast Guard conducts regular inspections, spot checks, and TWIC verifications at approximately 3,100 maritime facilities, 14,000 vessels, and 50 outer continental shelf facilities. The enforcement program also includes the use of hand held TWIC readers by Coast Guard personnel to conduct spot checks using the biometric capabilities of TWIC.

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

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

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

Promoting Preparedness

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

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

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

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

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

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

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

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

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

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

THE STRATEGIC CONTEXT

The National Strategy for Global Supply Chain Security

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

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

CHALLENGES AHEAD

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

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

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

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

Expanding Trade

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

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

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

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

Aging Infrastructure

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

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

International Trade Data System and Trade Facilitation

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

Perimeter Security

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

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

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

Cyber Security

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

CONCLUSION

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

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

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