CONSOLIDATED STATEMENTS OF

JAYSON P. AHERN
ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS
U.S. CUSTOMS AND BORDER PROTECTION

RDML CRAIG BONE
ASSISTANT COMMANDANT FOR PREVENTION
UNITED STATES COAST GUARD

MAURINE FANGUY
TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL
PROGRAM DIRECTOR
U. S. TRANSPORTATION SECURITY ADMINISTRATION

At the hearing before the House Homeland Security Subcommittee on Border, Maritime and Global Terrorism

26 April 2007

Introduction

The Department of Homeland Security appreciates this opportunity to discuss with you today the Security and Accountability For Every Port Act and the efforts of its components six months after its passage.

It is noteworthy that DHS, CBP, TSA, and the Coast Guard worked quite closely with the House and Senate in the development of the SAFE Port Act and applaud the high level of Congressional interest in securing United States ports and the global supply chain. Much of what is in the SAFE Port Act codified initiatives that the Department of Homeland Security undertook immediately after 9/11 and has been implementing successfully ever since.

Below are updates on the primary areas of activity being undertaken by the testifying components to fully implement the Act.

Area Maritime Security Plans.

Development of Salvage Response Plans within each Area Maritime Security Plan (AMSP) has been integrated into the five-year plan update cycle established by the Maritime Transportation Security Act (ACT) of 2002. The AMSP update will be performed by Federal Maritime Security Coordinators (FMSC) in consultation with their respective Area Maritime Security Committees (AMSC) and is planned for completion during early summer 2009.

A Salvage Response Plan will be a major element of the U.S. Marine Transportation System (MTS) recovery section of each AMSP and will provide the coordination and procedural foundation to support development of unified

command incident action plans under the Incident Command System (ICS) construct when salvage response becomes necessary to facilitate resumption of trade. Authorities, capabilities, and other salvage issues are currently being coordinated and researched with Federal Government partners. Consultation with national-level salvage industry representatives is continuing with the development and establishment of a Memorandum of Understanding (MOU) between the Coast Guard and the American Salvage Association of America. The MOU will establish a working partnership with goals of strengthening the communication and working relationship between the Coast Guard and the marine salvage and fire fighting industry to improve vessel and personnel safety within the industry, enhance national security preparedness and response, promote timely and professional salvage response to marine casualties, and enhance the protection of the environment along the nation's waterways.

Resumption of commerce and recovery of the marine transportation system (MTS) following a significant disruption is an issue of concern nationwide. The Maritime Transportation Security Act (MTSA) 2002 required that the National Maritime Transportation Security Plan include a plan to restore cargo flow following a National Transportation Security Incident (NTSI). The Coast Guard held a National Recovery Symposium at the National Maritime Institute of Technology and Graduate Studies on August 1st and 2nd, 2006. The symposium was attended by over 150 executive level participants from numerous branches of state and federal government, and the private sector.

The Coast Guard is currently developing a concept of operations and specific planning requirements and organizational structures to ensure a focus on MTS recovery following a significant incident that disrupts the MTS. MTS recovery guidance will be harmonized with, and support implementation of, the forthcoming Strategy to Enhance International Supply Chain Security that is being prepared by the Department of Homeland Security with Coast Guard and interagency input. Implementation guidance will also harmonize with MTS recovery principles gleaned from Hurricane Katrina lessons learned that have already been published in the U.S. Coast Guard Incident Management Handbook.

Review of maritime security developments since the implementation of MTSA, MTS recovery lessons from Hurricane Katrina, best Area Maritime Security practices from the field, and an update of MTSA implementation guidance are in progress. Review results will form the basis for revising Navigation Vessel Inspection Circular (NVIC) 09-02 which is used to guide the five-year AMSP update.

Consistent with the overriding requirement to deter, and when necessary, mitigate the effects of Transportation Security Incidents (TSI), the Coast Guard is working to make AMSP coordination and procedures hazard and transportation disruption compatible as much as practicable. This, in conjunction with oil and hazardous materials response coverage provided through Area Contingency Plans (ACP) and application of Incident Command System (ICS) principles and structures per the National Incident Management System (NIMS), is intended to

support a consistent preparedness approach across all transportation disruptions without the need for additional port-level plans.

Maritime facility security plans.

The Department of Homeland Security recognizes that information on ownership of maritime facilities and the companies that operate them is vitally important to the management of the security posture and the clear delineation of security responsibilities within the port. Currently, in 33 CFR 104.415(b)(2), 105.415(b)(2), and 106.415(b)(2), the Coast Guard requires a security plan audit whenever the owner or operator of a vessel, facility or Outer Continental Shelf (OCS) facility changes. Should the audit reveal that an amendment to the security plan is necessary, the security officer of the vessel, facility or OCS facility, will submit the amendment to the cognizant Captain of the Port or District Commander for approval. Consistent with the requirement in Section 102 of the SAFE Port Act, the DHS Appropriations Act of 2007 requires the Coast Guard to gather ownership information on vessel and facility security plans.

In order to meet the requirements in these statutes, the Coast Guard has initiated a regulatory project to update 33 CFR Subchapter H regulations and will incorporate these new ownership reporting requirements.

Implementation of the Transportation Worker Identification Credential (TWIC) regulations published in January 2007 will meet the requirement in Section 102 for a qualified individual having full authority to implement security actions for a facility. The Secretary can still waive the requirement after a determination based on a complete background check of the individual. These regulations in 33 CFR 105.205(a)(4), require facility security officers (the qualified individuals in the statute) to possess and maintain a TWIC. The security threat assessment conducted as part of the TWIC program includes a complete background check, including a criminal history records check, a legal status check, and an intelligence and terrorist watch list check, thus satisfying the relevant mandate within this section. In addition, the Coast Guard is addressing the requirement for Facility Security Officers to be U.S. citizens in the regulatory project to update Subchapter H.

Unannounced inspections of maritime facilities.

Currently, Coast Guard policy requires one annual inspection of each facility to be supplemented with periodic spot checks. The FY 2007 Homeland Security Appropriations Act provided $15M to, among other efforts, fund additional port security inspections. With this funding, the Coast Guard has created 39 new field billets, which will be filled during the 2007 transfer season, to add to the existing 350 facility inspectors. The Coast Guard has also created 61 reserve inspection billets to support additional inspections until permanent billets are filled this summer. This will ensure that each facility is inspected no less than two times per year, with at least one being an unannounced inspection. The Coast Guard conducted more than 7500 annual security inspections and unannounced spot checks of 3200 facilities in calendar year 2006, and will use the additional billets

to increase these inspections. The 2006 inspections resulted in 465 violations which levied $1,892,000 in penalties.

Transportation Security Card.

The final rule for TWIC went into effect on March 26, 2007. With the passing of this critical milestone, this hearing provides an excellent opportunity to highlight program developments and describe how the Department of Homeland Security is incorporating lessons learned into an effective, efficient business plan for TWIC enrollment. This extremely important program is moving aggressively towards its objectives with a focus on making good security and business decisions. This leading edge program is developing essential processes, capabilities and expertise that will be beneficial to other programs.

The Department of Homeland Security has framed the program decisions and processes within the context of the nation's port security goals, including the need to:

- Identify authorized individuals who require unescorted access to secure areas of Maritime Transportation Security Act (MTSA) regulated facilities and vessels;
- Determine the eligibility of an individual for access through a security threat assessment;
- Ensure unauthorized individuals are denied access through biometric confirmation of the credential holder;
- Revoke access promptly for individuals who fail to maintain their eligibility;
- Apply privacy and security controls to protect TWIC information; and,
- Fund the program entirely by user-fees.

Achieving these ambitious goals has required creative planning, flexible implementation, effective stakeholder communication, and adaptive contract management. The basic program deployment philosophy has been a commitment to evaluate all practicable technical alternatives that will provide adequate port security and minimize adverse impacts, either economically or logistically, to United States citizens and the international trading system. This has been and will continue to be the program's implementation premise.

The Department of Homeland Security fully respects the fact that this program has significant operational implications to the economic wellbeing of the nation. Therefore, the Department is committed to ensuring that the program is tested, fully integrated and does not compromise security in any linked system TWIC is an advanced, sophisticated credentialing system that presents at least four groundbreaking technological challenges:

- TWIC uses the latest, most advanced federal government biometric and credentialing standards and for the first time applies them to the commercial sector.

- TWIC issues cards that work anywhere in the nation's private port environment, involving multiple potential companies and industries, by anyone working in a secure area.
- TWIC has not only unparalleled flexibility, it involves mass scale. There will be over 750,000 card holders working at 3,200 ports.
- TWIC security checks will be integrated into all of TSA's vetting programs creating potential security synergies throughout the entire transportation sector.

In other words, the hard part is not the card; the challenge is the network behind the card. The landmark technical principle underlying TWIC's ability to authenticate a person's identity includes three factors. When using the full extent of TWIC's authentication ability each person can be identified by:

- Something they know – a worker's Personal Identification Number (PIN);
- Something they have – the TWIC credential; and
- Something they are – a biometric.

With these considerations in mind, the below provides an overview of milestones completed, program plans, and how the Department has incorporated the lessons learned from this pioneering program.

TWIC Milestones to Date.

Obviously, new processes and technologies require systematic pilot studies. The prototype study was deployed to 26 locations in the areas of Los Angeles/Long Beach, Wilmington/Philadelphia and Florida's deepwater ports. The prototype TWIC was successfully issued to more than 4,000 volunteer workers including truck drivers, longshoremen, container terminal, railway, and airport personnel. A name-based threat assessment was completed on each individual. A criminal background check was conducted by the State of Florida for the deep-water port volunteers. These efforts were a success on multiple levels; it provided invaluable experience and a much deeper understanding of the technical and logistical challenges.

Security improvements cannot wait until TWIC is fully deployed. The Department has gone forward with significant interim security enhancements and actions during TWIC's initial development phase. These actions included:

- The Coast Guard worked effectively with the National Maritime Security Advisory Committee (NMSAC) to define secure areas. This definition will have a direct impact on over 10,000 vessels and more than 3,200 facilities. These secure areas delineate where a TWIC will be required for unescorted access.
- The joint rulemaking process between the Coast Guard and TSA was accelerated resulting in TWIC Notice of Proposed Rulemaking (NPRM) being published on May 22, 2006.

- The Coast Guard and TSA worked with industry partners to develop an interim process that compares a worker's biographical information against terrorist watch lists and immigration databases.
- Facility owners, facility operators and unions submitted worker names, date of birth, and, as appropriate, alien identification number. To date TSA has completed 750,000 name based threat assessments on port workers and longshoreman. This task will be repeated this summer to keep the assessment fresh. These assessments are interim measures and do not include the criminal history records check or biometric credential that is part of TWIC.

TWIC Rule and Stakeholder Input.

The TWIC rule was posted on the TSA and Coast Guard websites on January 1, 2007, and published in the Federal Register on January 25, 2007. The rule is the result of extensive public involvement and interagency coordination. In addition to the direct involvement of the National Maritime Security Advisory Committee, TSA and the Coast Guard held four public meetings in Newark, NJ, Tampa, FL, St. Louis, MO and Long Beach, CA. Over 1,900 comments were received from workers, port owners and operators, small businesses and others affected by the new program. All comments were carefully considered and significant changes were made to the NPRM in the development of the Final Rule. These changes include:

- The Coast Guard and TSA delayed the requirement to purchase and install electronic readers to allow for additional field testing, technology improvements, and more public comment.
- An expedited interim threat assessment process was created for new hires so that they may go to work pending completion of the full threat assessment.
- Immigration requirements were expanded to permit certain Visa-holders who are prevalent in the maritime industry to apply for a TWIC.

The rule also meets SAFE Port Act requirements to concurrently process TWICs and merchant mariner's documents, and to include a provision to enable newly hired workers to begin working after TSA conducts an initial threat assessment. In addition, the TWIC NPRM and Final Rule include provisions that respond to comments received from workers subject to similar threat assessment programs. These include:

- Creating a new process where TSA can make a determination that a security threat assessment conducted by another government agency is comparable, eliminating redundancy and reducing costs for workers;
- Providing workers more time to apply for an appeal or waiver;
- Streamlining the process, jointly with the Coast Guard, for merchant mariner credentialing and ensuring that there was no duplication of requirements resulting from the TWIC process.

TWIC cards will be required not only for port facility workers, but for anyone who seeks unescorted access to secure areas of a MTSA regulated facility or vessel, regardless of frequency. The workers covered by this rule include certain truck drivers, rail employees, security guards, longshoremen, as well as all U.S. merchant mariners. TSA will use the time tested security assessment procedures and standards that are currently used for commercial motor vehicle drivers licensed to transport hazardous materials, known as Hazardous Material Endorsements (HME). In short, TWIC will be issued to workers who successfully complete a security threat assessment, which includes: (1) a check against terrorist watch lists, (2) an immigration status check, and (3) a FBI fingerprint-based criminal history records check.

TWIC Card Readers.

The TWIC rule does not currently include a requirement for owners and operators to use card readers. This was done as a response to important public comments received on the NPRM and concerns from Congress expressed in the SAFE Port Act. The card reader requirement is being formulated and coordinated by extensive technical input from industry and the public. In the interim, workers seeking unescorted access to secure areas will present their cards to authorized personnel, who will compare the photo, inspect security features on the card, and evaluate the card for signs of tampering. At facilities with various sophisticated access control systems, the magnetic stripe on the credential could be used to grant or deny access at entry gates. The Coast Guard will also institute periodic unannounced checks to confirm the identity of the holder of the TWIC.

The Department of Homeland Security will continue to work closely with all interested parties to address the ever evolving technology issues. The TWIC technical architecture is compatible with Homeland Security Presidential Directive (HSPD) 12 and Federal Information Processing Standards (FIPS) 201-1 requirements which provide an open standard that will ensure interoperability and real-time exchange for supply chain security cooperation between the Department and the private sector. The applicant's photograph, name, TWIC expiration date, and a unique credential number are printed on the card. An integrated circuit chip on the card stores two fingerprint minutia templates and a PIN as well as a digital photo of the applicant, the applicant's name, and card expiration. The embedded computer chip is capable of being read by both contact and contactless card readers and also contains the magnetic strip and linear bar codes.

In addition to previously conducted prototype testing, pilot test planning and discussions with interested port, facility, and vessel operators began late last year. The pilots will test access control technologies in real world marine environments. The National Maritime Security Advisory Committee is providing invaluable input regarding operational requirements and has recommended specifications for contactless biometric smart cards and card readers. Public feedback is being collected and analyzed on the recommendations. As part of the outreach efforts for the TWIC program and the Department's Port Security

Grant Program the Department has met with a number of maritime interests to invite their participation in the pilot tests. The Department's objective is to include pilot test participants that are representative of a variety of facility and vessel types and sizes which operate in a variety of geographic locations and environmental conditions. There appears to be sufficient interest from the maritime community to achieve this objective.

The Department of Homeland Security is currently reviewing Port Security Grant applications relating to these pilot studies and will announce awards later this spring. While the grant process is proceeding, TSA and the Coast Guard are working with Department test and evaluation experts to develop a comprehensive plan that addresses the unique pilot test challenges. The evaluation of the pilot tests will greatly facilitate the Department's efforts to propose a TWIC reader requirement rule that effectively addresses security requirements, maintains the flow of commerce, and protects the personal information used to validate the TWIC holder's identity.

Rollout Contract.

A key operational piece of the rollout plan was the award of a competitively bid, indefinite delivery/indefinite quantity contract to Lockheed Martin Corporation. The TWIC enrollment and systems operations and maintenance contract will include a Quality Assurance Surveillance Plan (QASP) that establishes detailed metrics to be monitored through the life of the contract and will determine whether the contractor will receive any award fee for services performed.

Lockheed Martin will establish approximately 130 enrollment centers near the port facilities where applicants will provide biographic information and fingerprints. This information will be transferred to TSA so they may conduct a threat assessment involving checks of criminal history, immigration, and intelligence databases. Once a worker successfully completes the threat assessment process, the government will produce the credential and send it to the enrollment center, where the worker will retrieve it. TWIC enrollment will begin initially at select ports based on risk and other factors and will proceed throughout the nation over the next 18 - 24 months.

TWIC Card Costs.

As required by Congress, the costs of the program will be borne by TWIC applicants. Therefore, the Department is obligated to look for practicable ways of controlling costs, eliminating duplicative processes, providing timely decisions, and, most importantly, ensuring accuracy and fairness.

The fees for a TWIC will be slightly lower than was anticipated in the Final Rule. A TWIC will be $137.25 for a card that is valid for 5 years. Workers with current, comparable background checks (e.g., HAZMAT, Merchant Mariner Document (MMD) or Free and Secure Trade (FAST)) will receive a discounted fee of $105.25. The cost of a lost, damaged or stolen credential is $36, although the Department has solicited comment on raising that fee.

The Department of Homeland Security fully realizes that these costs are not an insignificant amount to some workers. However, the Department feels that the costs compare very favorably with equivalent HSPD-12 compliant card fees and in some instances may actually reduce the costs for some workers. For example, the Coast Guard is in the process of completing a companion rule which will consolidate existing mariner credentials and streamline the application process for mariners who have already applied for the TWIC. This will reduce the overall cost burden for these workers. Preparations are underway to reduce duplication by having TSA provide the Coast Guard with electronic copies of the applicant's fingerprints, proof of identification, proof of citizenship, photograph, and if applicable the individual's criminal record, FBI number and alien registration number. This will eliminate the need for TWIC holding mariners to visit a Coast Guard Regional Exam Center to apply for or renew their Merchant Mariner Credential unless an examination is required.

Rollout Communication Plan and Pre-Enrollment.

Effective public communication is fundamental to the Department rollout plan. The TWIC program office has used the lessons learned from the prototype phase to develop a multi-dimensioned outreach strategy for all of the enrollment phases. A toll-free help desk, Frequently Asked Questions, informational brochures, and a centralized e-mail address will provide up-front assistance and guidance for workers, owners, and operators. These services include program information, response to enrollment questions, pre-enrollment assistance, lost/stolen card reporting, credential replacement support, updates on an individual's case, and information on appeals and waivers. Applicants are encouraged, but not required, to "pre-enroll" and provide biographic information at the secure TWIC web site which should help reduce waiting time at the enrollment centers. An additional service that is provided during pre-enrollment is an opportunity for the applicant to schedule an appointment for appearing at the enrollment center.

Lockheed Martin is required by contract to develop a communication plan to ensure that applicants, operators, and relevant industry associations are educated and knowledgeable about the TWIC enrollment process. The communication plan will identify TSA goals and responsibilities, contractor goals and responsibilities, port facility and vessel responsibilities, target audiences, communications processes, and supporting communication tools. A key plan element was the establishment of the TWIC Stakeholders Communications Committee. The initial committee meeting was held last month with new meetings on a regularly occurring basis. These meetings will serve as a forum to ensure sustained two-way communication with stakeholders and directly provide the most current, accurate program information. Additionally, Lockheed Martin will facilitate rollout communications by deploying advance teams prior to the opening of enrollment centers to seek input and communication from local port officials, field federal agents, and local stakeholders.

Enrollment Centers.

Enrollment sites will be operated by trusted agents who are employees of a vendor under contract with TSA. These trained agents will have undergone a TSA security threat assessment before being allowed to collect data. The trusted agents will provide applicants with a privacy notice and consent form, by which the applicant agrees to provide personal information for the security threat assessment and credential. The trusted agents will verify an applicant's identity, confirm the accuracy of biographic information, collect biometric information (a full set of fingerprints and a facial photograph), and obtain the applicant's signature on the enrollment documents. The contract performance parameter for the trusted advisor enrollment process will be an average enrollment time of 15 minutes. The enrollment process for a pre-enrolled applicant is fully expected to take less time. Focused planning that fosters convenience for applicants will benefit workers as well as garner process efficiencies.

Data Security Vetting and Card Issuance.

After enrollment, an applicant's data is sent to the TSA system, and the vetting process (i.e., terrorism database, criminal history records check, immigration check) is started. One of the top technical challenges to introducing the new technology associated with TWIC is ensuring that the data is appropriately and efficiently transmitted to the appropriate destinations. The Department intends to enhance security synergies and efficiencies by using the same screening IT systems used for security screening in other programs. These efficiencies, however, require the Department to be absolutely certain that the stability or security of this larger vetting system is not jeopardized. Rigorous performance testing, and the accompanying scheduling complexities, is the only way to know for certain that satisfactory technical integration has been achieved.

Once the technical integration has occurred, it is anticipated that the TWIC threat assessment processing time will be similar to that experienced in the HME program. Since the inception of the HME program, threat assessments have frequently been completed in 3 days or less. During this same period the average time for completing HME threat assessments has been approximately 14 days, which includes all appeals and waivers. The process will be impacted by steps where there is minimum governmental control. For example, applicants need to promptly provide corrected records, and respond to initial determinations. Other anticipated factors that could result in processing delays include an applicant providing incorrect information, watch list determinations, evaluation of the nature of threats, whether the applicant is currently under criminal investigation, and confirming immigration status that is not available in electronic format. Nonetheless, the 14 day average for processing the HME assessments includes the time required to meet the same threat assessment challenges that will be faced with TWIC.

If TSA determines that an applicant does not pose a security threat, the applicant's information is sent for card production. After the card is developed it is sent to the enrollment center, where the worker will be notified to pick up the card. Due to the secure nature of the credential, the smart cards are shipped as "inactive." An applicant must verify his or her personal identity by providing a

biometric (i.e., fingerprint) that is matched to the cards electronic template. After identity is verified, the applicant selects a secret PIN which is stored on the card as an additional identity authentication factor.

Worker Redress/Waivers/Appeals.

If an applicant is denied a TWIC they will be notified of the reason and instructed on how to apply for an appeal or waiver. All applicants have the opportunity to appeal a disqualification and may apply to TSA for a waiver..

The standards for denial of a TWIC are the same standards that apply in the HME process. Any applicant who is subject to removal proceedings or an order of removal under the immigration laws of the United States is not eligible to apply for a TWIC. An individual will be disqualified if he or she lacks legal presence and/or authorization to work in the United States, has a connection to terrorist activity, or has been determined to lack mental capacity.

A person will also be denied a TWIC for a criminal history involving certain disqualifying crimes. TSA received valuable NPRM comments on the list of disqualifying crimes and decided to fine tune the list to better reflect crimes that are more likely to result in a terrorism security risk or a risk that the individual may engage in a transportation security incident. Permanent disqualifying criminal offenses include: espionage, sedition, treason, terrorism, improper transportation of a hazardous material, unlawful possession, use or sale of an explosive, murder, threats to a place of public use (government facility, public transportation system, or infrastructure facility), violations of the Racketeer Influenced and Corrupt Organizations (RICO) Act in which the predicate act is one of the permanently disqualifying crimes, or a crime involving a transportation security incident. A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

Individuals are ineligible for a TWIC if convicted in the last seven years or incarcerated within the last five years of the following crimes: Unlawful possession, use or sale of a firearm or other weapon, extortion, fraud, bribery, smuggling, immigration violations, distribution or importation of a controlled substance, arson, kidnapping or hostage taking, rape or aggravated sexual abuse, assault with intent to kill, robbery, RICO violations that do not involve a permanent disqualifying crime.

The appeal process involves ensuring that the information on which TSA bases its threat assessment is completely accurate. This process allows the applicant to correct the record on which that threat assessment occurs.

Fairness and accuracy in TWIC waiver determinations are further ensured by an opportunity for independent review by an Administrative Law Judge. As previously noted, the regulations provide a lengthened period for appealing denial of waivers, from 30 days to 60 days, to accommodate workers who tend to travel for extended periods of time. Furthermore, the regulations allow a worker to file a request for a time extension after the deadline has passed by filing a

motion describing the reasons why they were unable to comply with the timeline. The extra procedural measures are intended to give workers every reasonable chance to bring legitimate concerns and issues to the attention of people who are trying to make the best and correct decision regarding security risks.

Lessons Learned and Future Efforts.

The initial rollout of TWIC will be focused on the maritime mode. However, once the initial maritime rollout is complete the Department of Homeland Security will evaluate deployment of this program in other modes of transportation. The analysis and planning for any resulting decision will benefit from the experience, technical expertise, and lessons learned that evolved under the TWIC program.

There are several vital lessons learned during the development of this program that must be prominently considered in future efforts:

- *Look for efficiencies in duplicative regulatory processes.* As noted previously, TSA and the Coast Guard are developing procedures for the sharing of mariner fingerprints, identity verification, criminal history, and photographs for TWIC which is expected to save not only money but time. In addition, merchant mariners will no longer be required to visit a Regional Exam Center to obtain and renew their credentials, resulting in substantial time and travel savings.
- *Address the impact on small businesses.* TSA and the Coast Guard worked closely with the Small Business Administration to minimize the financial and operational impact on small businesses wherever possible. The rule includes provisions that allow MTSA-regulated passenger vessels (excluding cruise ships) to establish employee access areas for crewmembers that do not require unescorted access to secure areas such as the pilot house and engine room. This provision reduces the impact on those employees who rarely need to use spaces beyond those designated for support of passengers while maintaining the integrity of vessels' secure areas. A Small Business Compliance Guide is also being produced and distributed to assist small businesses in their implementation of the program.
- *When practicable, preserve State regulatory flexibility.* Mariner regulations and port security plans preempt state regulations. However, TSA does not preempt States from requiring background checks and badging systems in addition to TWIC. States may need to set standards for important purposes other than terrorism threats.
- *Plan for privacy.* All data collected at an enrollment center will be deleted from the enrollment center work stations. The entire enrollment record (including all fingerprints collected) is stored in the TSA system, which is protected through role-based entry, encryption, and segmentation to prevent unauthorized use. No paper records are created during the enrollment process.

- *Technical innovation requires adaptive contract management.* TWIC is attempting to develop a 21st century technology that accommodates evolving IT standards suited to emergent needs that span local, international, public, and private interests. This requires continual reevaluation of the scope and methods of contracting. The recent Lockheed Martin contract award is a culmination of Department efforts to date. Due to the nature of this task, however, the Department will need to continue to look for and implement adaptive planning, metrics, and changes to ensure this effort stays on track.
- *Don't expect a "silver bullet" technology solution.* Evolving technology, such as card readers, creates a changing environment and program control constraints. This is especially the case when the technology must be deployed to a vast multitude of entities with remote connectivity challenges (e.g., vessels) and varying degrees of access control system capabilities.
- *Place the highest value in stakeholder input; it is time well spent.* The public hearings, comments to the NPRM, meetings with operators and associations, and contributions of advisory councils all added pure value. The Department came away from each and every one of these efforts better informed about the challenges, the unacceptable impacts, and the practicable options for protecting United States ports.

Long-range vessel tracking.

The Coast Guard currently meets the intent and tracking requirements of the Act using the full range of classified and unclassified vessel tracking information available. However, it takes up to two years to develop and finalize a regulation, and the Long Range Identification and Tracking (LRIT) NPRM is still being developed and, therefore, did not meet the April 1, 2007 deadline. The Act requires the Secretary of the Department of Homeland Security to establish a long range automated vessel tracking system that meets the following:

- *Tracking*: Provided for all vessels in U.S. waters equipped with Global Maritime Distress and Safety System (GMDSS) or equivalent satellite technology
- *International*: Consistent with international treaties, conventions and agreements

Tracking:

The SAFE Port Act requirement demands a multi-faceted approach. Using the full range of classified and unclassified vessel tracking information, including some information purchased from vendors where appropriate, the Coast Guard currently meets and exceeds the tracking requirement of the Act. Currently, sufficient tracking information exists, but work is needed in the processing, display, and training in the use of this information.

International:

The Departments work to establish a system through the International Maritime Organization (IMO) will provide an unclassified global tracking capability by the end of 2008 as a part of recently adopted amendments to an existing IMO convention and make available to the United States a system that is compatible and interoperable with the global maritime community. Since shortly after 9/11, the Coast Guard has been working with the IMO to implement a global tracking system for the types of vessels described in the Act. Following considerable U.S. diplomatic efforts, the international agreement to implement such a system was reached last year, and the global tracking system will be in effect at the end of 2008. In the long run, this approach is more advantageous to the United States because it applies globally to all ships described in the Act rather than just those in U.S. waters or vessels intending to make port calls in the U.S. Under this system, the U.S. will have access to information for U.S. Flag vessels regardless of their current location and vessels bound for U.S. ports when they declare intent to arrive. Information on all other vessels will be available whenever a ship is within 1,000 nautical miles of the U.S. coast. The Coast Guard is examining funding strategies for this important international system that it is committed to support, and believes it will be able to implement capabilities to participate by the time the system comes into effect.

Interagency operational centers for port security.

Section 108 requires a budget and cost-sharing analysis for implementing interagency operations centers. The Department of Homeland Security did not meet the April 11, 2007 report deadline because it is are still working with agency partners to provide a consistent report. An interim letter has been sent, indicating that the report will be completed by July 30, 2007.

The establishment of interagency operations centers is currently not funded. In cooperation with Department of Justice (DOJ), Navy, and DHS Office of Science and Technology (S&T), three prototype centers have been established to date. The Coast Guard pilot projects for interagency operations centers are listed below. These centers are each configured differently as test beds for concepts, tactics, procedures and equipment. Cost sharing arrangements exist among the various participants.

Designator	Location	Cost-Sharing Agencies
Seahawk Joint Task Force	Charleston, SC	Dept. of Justice/U. S. Coast Guard
SCC*-Joint	Hampton Roads, VA	U. S. Coast Guard /U.S. Navy
SCC-Joint	San Diego, CA	U. S. Coast Guard /U.S. Navy

*Sector Command Center

Additionally, a half dozen locations have been identified for short and medium term pilot projects to develop joint operations design models between the Coast Guard and Customs and Border Protection (CBP). These pilots will include

examination of methods for implementation of a virtual command center constructs using collaboration tools.

When funded, the Command 21 project will field the capabilities necessary to create interagency operations centers as required by Section 108. This major establishment of proposed interagency operational centers for port security is a major system acquisition designed to close gaps in port and coastal maritime security.

Command 21 will:

- Improve maritime port and coastal security systems to complement the terrestrial Secure Border Initiative (SBI) Net;
- Improve unity of effort in a multi-agency operations center environment;
- Accelerate deployment of a net-centric tactical system that implements Department enterprise standards for the sharing of situation data and services across multiple Department interagency domains and Coast Guard systems; and
- Help address the security and safety issues posed by the 17 million smaller vessels that operate in port and coastal areas.

The Coast Guard's experience with interagency operations centers demonstrates that many tangible benefits to improve maritime safety, security, and stewardship can be achieved. Some of these include:

- Facilitate cooperative targeting and coordination of intelligence;
- Daily field-level coordination that breaks down barriers between agencies;
- Collective use of tactical sensors (radars/cameras) saves time, money and effort;
- Cooperative planning that improves readiness and efficiency; and
- Sharing of law enforcement information that helps reduce criminal activity in the port and cut off potential funding to terrorist groups.

Command 21 will close a critical gap between current capabilities and the desired interagency end state. Future interagency operations will be greatly improved as all partners will be able to:

- **See** maritime activities using port surveillance sensors;
- **Understand** the scene by automatically bringing tactical and intelligence information together; and
- **Share** this tactical data with each other as they work side by side in improved facilities.

Command 21 will publish tactical data in an open standard that allows other systems across multiple Department domains to subscribe to the information and use it according to the individual needs of each agency. It provides the maritime

component of the Department of Homeland Security's Secure Border Initiative (SBI). Good government demands that both programs move forward in parallel to increase deterrence capabilities. If the two programs move ahead unevenly, illegal incursions will seek the path of least resistance. Moving ahead on both fronts will provide collaborative opportunities to leverage critical resources to broaden the impact of both programs toward securing the borders.

Notice of arrival for foreign vessels on the Outer Continental Shelf.

The regulations for Notice of Arrival for Foreign Vessels on the Outer Continental Shelf (OCS) are being developed and incorporated into an existing Coast Guard rulemaking project related to OCS activities. This rulemaking, the updating of 33 CFR Subchapter N, "Outer Continental Shelf Activities," already includes Notice of Arrival requirements for foreign vessels operating on the OCS. Once the Coast Guard has completed evaluation of the proposed regulations and public comments, the final rule will be issued to implement the provisions of Section 109 as expeditiously as possible.

Enhanced crewmember identification.

Historically, the Coast Guard advanced the effort to negotiate the international seafarer's identification initiative at the International Labor Organization (ILO), resulting in the ILO-185 Seafarer's Identification Document (SID). However, a requirement within ILO 185 prohibiting implementing nations from requiring a visa for seafarers holding a SID to be eligible for shore leave has prevented the U.S. from ratifying ILO 185.

The Coast Guard is engaged in discussions with Customs and Border Protection (CPB), Department of State, and Department of Labor to evaluate all options. In accordance with the Act, the Coast Guard will initiate a rulemaking to define identification documents necessary for foreign mariners calling on U.S. ports.

Risk assessment tool.

The Maritime Security Risk Analysis Model (MSRAM) is being used by Captains of the Ports/Federal Maritime Security Coordinators and Area Maritime Security Committees (AMSC) to analyze and prioritize scenario-based risks within their areas of responsibility and measure risk reduction potential in the evaluation of port security grant program proposals. AMSCs are required to validate the MSRAM on an annual basis. This was last completed in 2006 using MSRAM Version One, with an update expected to be complete in the summer of 2007 using MSRAM Version Two.

Port security grants.

The Coast Guard has been working with Department of Homeland Security Office of Grants and Training, who has fiduciary responsibility for the Port Security Grant Program, to complete the report to Congress required by this Section, but the report is not yet complete. In the interim, a letter was sent to Congress stating that the April 11, 2007 deadline would not be met but that the Department expects to have the report to them by July 30, 2007.

The Port Security Grant Program (PSGP) provides grant funding to port areas for the protection of critical port infrastructure from terrorism. Fiscal Year 2007 PSGP funds are primarily intended to assist ports in enhancing risk management capabilities, domain awareness, capabilities to prevent, detect, respond to and recover from attacks involving improvised explosive devices (IEDs) and other non-conventional weapons, as well as training and exercises.

The total PSGP funding available in Fiscal Year (FY) 2007 is $201,670,000, and these funds were divided into four tiers of ports. Within Tier I, eight of the highest risk port regions have been identified and are eligible to apply for a fixed amount of funding based on risk. In many cases, multiple port areas have been grouped together to reflect geographic proximity, shared risk, and a common waterway. Port areas submitting applications within Tier II and III are eligible to compete for the FY07 PSGP but are not guaranteed funding. Section 112 of the Act also required that any entity addressed in an Area Maritime Security Plan also be eligible to apply. Tier IV has been established for those new entities not within the port areas in Tiers I-III. This added approximately 259 ports to the 102 highest risk ports for a total of 361 that are eligible to compete with no guarantee of funding.

Funds will be awarded based on analysis of risk and the effectiveness of the applicants' proposed investments. Risk to port Infrastructure Protection Program Detail areas is assessed using a methodology consisting of threat, vulnerability, and consequence factors. The majority of port security grant funds – $120.6 million – will be available to eight Tier I ports or port areas considered to be the highest risk.

Grant applicants had 60 days from January 6, 2007 to complete this process for the remaining $81M. Applications were required to be submitted electronically via the grants.gov web site no later than 11:59 PM Eastern Standard Time on March 6, 2007.

The initial reviews were completed by the local Captain of the Port and results were forwarded to a national review panel comprised of representatives from the Coast Guard, the Transportation Security Administration (TSA), The Department of Homeland Security Infrastructure Protection (IP), Grants and Training (G&T), the Domestic Nuclear Detection Office (DNDO), and the Maritime Administration (MARAD) that convened for two weeks beginning April 9, 2007. It is anticipated that awards will be announced in the beginning of May 2007.

Port Security Training Program.

The Coast Guard is supporting the FEMA National Preparedness Directorate's National Integration Center, through Training and Exercises Integration (formerly a function of the Preparedness Directorate, Office of Grants and Training Division) in implementing the requirements of the Act relating to Port Security Training. Collectively, progress has been made in establishing the program delineated in the Act, and there are a number of existing initiatives and new initiatives that taken together will address the requirements.

In response to Congressional mandate, the Coast Guard and MARAD prepared a Report to Congress and developed model courses for the training of facility and other personnel to meet the requirements in Section 109 of the Maritime Transportation Security Act of 2002. These model courses establish a competence-based standard and contain the majority of the requirements under this Section of the Act. The model courses were developed in support of the facility security plan requirements and apply to all personnel working in a port facility or required to enter a port facility in response to an emergency. These model courses are currently available via the MARAD website to Federal, state and local personnel from the public and private sector, and they are undergoing a review to include lessons learned and the additional topics required under the Act. To ensure quality training, Coast Guard and MARAD developed and implemented a voluntary course approval and certification process using the model courses as the guidelines for acceptance. The CG is currently revising the regulations for security training for facility personnel to ensure that all training is measured against a standard of competence, including the topics required under by the SAFE Port Act.

The FEMA National Preparedness Directorate's National Integration Center, through Training and Exercises Integration, has awarded a $6.18 million Cooperative Grant to the Florida State University to develop courses meeting the Maritime Transportation Security Act of 2002 requirements (model courses) and covering the eight port security-related topics required under the Act. MARAD and the USCG are actively assisting DHS to ensure that this training will be consistent with existing standards and that it will provide the maximum possible return on investment. It is envisioned that these courses will be available for in-classroom and on-line training, and will be available to Federal, state and local personnel as well as to members of the private sector who work in the port security realm.

In addition, the FEMA National Preparedness Directorate's National Integration Center, through Training and Exercises Integration, has available other training courses that address individual port security topics required under the Act. These courses are provided to State and local emergency responders and other identified audiences by Training and Exercises Integration, and coordinated by each State's governor-designated Training Point of Contact.

Port Security Exercise Program.

Current port security exercise programs conduct live risk-based exercises that are realistic and evaluate total capability by focusing on the port community. These exercises involve State and local governments, as well as facilities and vessels, to ensure that consistent methodology is applied and that all requirements are met as a result. Although current programs do not mandate facility participation in these annual exercises, participation has been strong and continues to increase. Facilities, as well as vessels, are encouraged to observe and/or participate in these port security exercises. When they choose to participate, they are offered the opportunity to put forth exercise objectives tailored to meet their specific needs.

Since January 2005, the Coast Guard has assisted TSA in implementing their Port Security Training and Exercise Program (PortSTEP). Similarly, since October 2006, the Coast Guard has sponsored its own Area Maritime Security Training and Exercise Program (AMStep) that exercises the port stakeholder's ability to execute the Area Maritime Security Plan. The Coast Guard and TSA have synchronized AMStep and PortSTEP to maximize coverage across the U.S. and minimize duplication of effort. In calendar year 2006, these two programs collectively sponsored 53 port security exercises. The results of both these exercise programs and all lessons learned, best practices and corrective actions are documented in a semi-annual report to Congress. Exercise types have included basic and advanced table-top, discussion-based exercises to full-scale, operations-based exercises. The type of exercise and scenario selected are collectively decided upon by Area Maritime Security Committee (AMSC) members, through application of their most current risk-based port assessment.

The "Training" aspect of current port security exercise programs focuses on the National Incident Management System (NIMS) Incident Command System (ICS). Training, such as I-200 (Basic), I-300 (Intermediate) and I-320 (Team training), and is offered to the entire port community prior to each annual exercise. Security-specific training is provided from within the port community.

Initial performance measures for port security exercises were established under change two to Coast Guard NVIC 09-02. These measures, outlined as objectives, are currently being revised by the Coast Guard Office of Incident Management Preparedness to align with the Department of Homeland Security Preparedness capabilities-based planning model. All lessons learned and best practices are captured in the Coast Guard Contingency Preparedness System (CPS), which can be accessed by the entire Coast Guard. Additionally, through the use of Homeport, the Coast Guard's web-based communications and collaborations Information Technology application, Lessons Learned & Best Practices are made available to the entire port community (Federal, state, local, tribal and industry). Finally, the Coast Guard is working with the Department to offer and post select After Action Reports to the Department Lessons Learned Information Sharing (LLIS) system.

The implementation of the Coast Guard Remedial Action Management Program (RAMP) in May 2006 has assisted in the tracking and correction of numerous issues identified through current port security programs.

Although AMStep is currently being carried out under contract support, the Coast Guard has begun the hiring of personnel to staff National-level and Regional-level exercise support teams. These teams will assist Coast Guard Sector Commands (port-level) and Districts with the following contingency exercise programs: port security, oil/hazardous substance response, natural disaster, mass rescue, alien migration interdiction, civil disturbance, counterterrorism, military outload, combatant commander support, and physical security/force protection. This is an "All Threats / All Hazards" approach.

Facility exercise requirements.

Current regulations in 33 CFR 105.220(c) require facilities to conduct an annual exercise. These exercises may include either live, tabletop, or participation in a non-site-specific exercise. In order to meet the requirement in Section 115, the Coast Guard has initiated a regulatory project to update 33 CFR Subchapter H regulations and will incorporate the definition of "high risk facility" and the requirement for high risk facilities to conduct annual full-scale exercises.

Domestic radiation detection and imaging.

The SAFE Port Act requires that a deployment strategy plan be developed for the placement of radiation portal monitors (RPMs) throughout the nations ports of entry. That plan has been recently submitted to Congress by the Department.

CBP began deploying RPMs in October 2002, with the first deployment at the Ambassador Bridge in Detroit. Since that time, CBP and the Domestic Nuclear Detection Office (DNDO) have deployed 973 RPMs at mail facilities, seaports, and land border crossings, and will deploy the first RPM in the air cargo environment this year. Specifically, the SAFE Port Act mandates that all containers entering through the top 22 seaports be scanned for radiation. Currently, the Department has deployed radiation detection equipment to each of these 22 ports. Due to unique operational considerations at some of these ports, not every terminal within a port is currently equipped with such equipment. However, to satisfy the requirements of the SAFE Port Act and to further enhance port security, CBP and DNDO continue to work with these considerations, and by the end of this calendar year will scan 98% of all containerized cargo at these 22 seaports. With the additional deployment of radiation screening equipment CBP currently scans 91% of the cargo and 81% of the passenger vehicles arriving from Canada; 96% of the cargo and 91% of the passenger vehicles arriving from Mexico, as well as 89% of arriving sea-borne cargo containers.

Since CBP began scanning cargo and conveyances for radiation, they have scanned over 151 million conveyances, and resolved over 840,000 alarms. This is a tremendous workload, and the SAFE Port Act authorizes 200 new CBP Officers in each of the next five years to help accomplish this mission. Furthermore, the Department is currently testing the next generation of radiation detection equipment known as Advanced Spectroscopic Portals at the New York Container Terminal (NYCT). Future deployments of ASPs will allow CBP to quickly differentiate between benign materials such as kitty litter or granite, while determining which shipments pose a true risk. This will perfectly fit with CBP's twin goals of increasing security while facilitating the flow of legitimate trade and people.

Inspection of car ferries entering from abroad.

CBP is currently developing a plan for the inspection of passengers and vehicles on ferries before the ferry embarks for the United States. Ferries reach the United States from four countries: Mexico, Canada, the Dominican Republic, and the British Virgin Islands. Currently, CBP is in the process of contacting the owners and operators of each ferry with a U.S. arrival to help determine the level

of interest and the proper course of action. Once feedback from the owners and operators is received, CBP will reach out to the foreign governments of Mexico, Canada, the Dominican Republic, and the British Virgin Islands to further collaborate on implementing a plan.

Center of excellence for Maritime Domain Awareness.

The Coast Guard is assisting the Department of Homeland Security Science and Technology (S&T) Directorate to meet the requirements of the Act relating to a Center of Excellence for Maritime Domain Awareness (MDA). The Broad Area Announcement (BAA) for a Center of Excellence (COE) for Maritime, Island and Extreme/Remote Environment Security was announced at the beginning of February 2007. This BAA incorporated MDA study as a central component of a broader system of research into maritime security. This solicitation is still open, and there has been a promising response from the academic community. S&T expects to award the COE by the end of 2007. The Coast Guard looks forward to this important new research component that will support DHS.

Security of the International Supply Chain

The SAFE Port Act requires the Department of Homeland Security develop and implement a strategic plan to enhance the security of the international supply chain, including protocols for post-incident resumption of trade. A working group consisting of Department component subject matter experts was convened shortly after enactment and completed drafting the strategy in early February. The Department is currently consulting with appropriate groups including the Federal Interagency and Federal Advisory Committees and is on track to finalize the document and meet the July 10, 2007 submission deadline.

Automated Targeting System.

CBP requires advanced electronic cargo information as mandated in the Trade Act of 2002 (including the 24-hour rule for maritime cargo). Advanced cargo information on all inbound shipments for all modes of transportation is effectively evaluated using the Automated Targeting System (ATS) before arrival in the United States. The SAFE Port Act requires CBP to seek additional data elements for ATS as well as to evaluate the entire system. CBP is complying with both these mandates

As a matter of background, ATS provides decision support functionality for CBP officers working in Advanced Targeting Units (ATUs) at United States ports of entry and CSI foreign ports. The system 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. ATS uses a rules-based program to highlight potential risk, patterns, and targets. Through rules, the ATS alerts the user to data that meets or exceeds certain predefined criteria. National targeting rule sets have been implemented in ATS to provide threshold targeting for national security risks for all modes: sea, truck, rail, and air.

Working with the Commercial Operations Advisory Committee (COAC), CBP has proposed a new Security Filing in an effort to obtain additional advanced cargo information and enhance their ability to perform risk-based assessments prior to cargo being laden on a vessel overseas. The CBP proposal, better known as "10 plus 2" covers the following key areas:

- Ten unique data elements from importers not currently provided to CBP 24 hours prior to the foreign loading of cargo;
- Two additional data elements provided by the carriers including the Vessel Stow Plan which is currently utilized by the vessel industry to load and discharge containers and Container Status Messaging which is currently utilized by the vessel industry to track the location of containers and provide status notifications to shippers, consignees and other related parties.

CBP is currently developing a Notice of Proposed Rulemaking (NPRM) which will be published in the Federal Register along with a request for comments. Obtaining additional information earlier in the process will increase the transparency of the global supply chain enabling the refinement of CBP's targeting processes and will provide additional information to make a more fully informed decision with respect to the risk of individual shipments.

In addition to Security Filing, CBP continually updates ATS. Since 2004, ATS has continually undergone independent audits from the GAO and the IG. Furthermore, CBP regularly reevaluates to improve the data sets in ATS. The Office of Field Operations National Targeting and Security (NTS) office and the Office of Information Technology Targeting and Analysis Systems Program Office (TASPO) have been working together to enhance the ATS Maritime rule set capabilities for ocean cargo targeting. Under the direction of OFO, TASPO placed the updated rule sets into production on March 21, 2007, to conduct initial assessments. Since that time, OFO subject matter experts and members of the Maritime Targeting Working Group have provided feedback to NTS, which resulted in further refinements and enhancements to the maritime rule set. Currently NTS is modeling several versions of the new Country of Interest list to include iterations of different scores and scenarios to include entity concepts such as first time, unknown, and high volume. OFO is currently using the updated rule set (OCEN5) for maritime threshold targeting.

Container security standards and procedures.

The Department of Homeland Security strongly supports and continues to seek opportunities to enhance supply chain security efforts, including enhancements to the security of the container. Indeed, securing the container is a critical part of a multi-layered approach to supply chain security. However, in order to establish minimum standards for container security, it is first necessary to ensure that there are available solutions that would significantly improve container security without significantly disrupting the flow of legitimate commerce. The Department does not believe that, at the present time, the necessary technology exists for such solutions. The Department is actively working with industry to test different

technologies and methodologies that would provide economically and operationally viable enhancements to container security.

It should be noted that minimum security criteria for participants in the C-TPAT do include a requirement that all C-TPAT importers must affix a high security seal to all loaded containers bound for the United States. These seals must meet or exceed the current ISO/PAS 17712 specifications for high security seals.

Container Security Initiative.

To meet their priority mission of preventing terrorists and terrorist weapons from entering the United States, CBP has partnered with other countries through their Container Security Initiative (CSI). CSI is another example where the SAFE Port Act codified existing DHS programs, and CBP is in compliance with the Act's mandates.

Almost 32,000 seagoing containers arrive and are off loaded at United States seaports each day. In fiscal year 2006, that equated to 11.6 million cargo containers annually. Because of the sheer volume of sea container traffic and the opportunities it presents for terrorists, containerized shipping is uniquely vulnerable to terrorist exploitation. Under CSI, which is the first program of its kind, CBP is partnering with foreign governments to identify and inspect high-risk cargo containers at foreign ports before they are shipped to United States seaports and pose a threat to the U. S. and to global trade.

The goal is for CBP's overseas CSI teams to conduct 100 percent manifest review before containers are loaded on vessels destined for the United States. However, in those locations where the tremendous volume of bills does not allow for the overseas CSI team to perform 100 percent review, CSI targeters at the National Targeting Center provide additional support to ensure that 100 percent review is accomplished. Utilizing the overseas CSI team and the CSI targeters at the National Targeting Center, CBP is able to achieve 100% manifest review for the CSI program.

Oversight of the CSI program is supported by automated tools for statistical analysis, an evaluation database to track and analyze any deficiencies identified during the evaluation process of the CSI ports, and a non-intrusive inspection (NII) equipment utilization database that tracks the use of NII equipment at CSI ports to include the downtime of the equipment.

Today, CSI is operational in 50 ports covering 82 percent of the maritime containerized cargo shipped to the United States. CBP is working towards strategically locating CSI in additional locations focusing on areas of the world where terrorists have a presence. CBP projects that by the end of 2007, CSI will be operational in 58 foreign seaports, covering over 85 percent of cargo destined for the United States. Declarations of Principles for each of the remaining 8 ports have been signed.

Customs-Trade Partnership Against Terrorism

The SAFE Port Act not only legislatively recognized the supply chain security industry partnership program known as C-TPAT, but the Act also added greater

accountability by mandating that certain program activities be completed within specific time frames, and that greater program oversight be developed for the program. CBP began implementing such changes, which were first outlined in GAO reports from 2003 and 2004, eighteen months prior to the passage of the Act, and continues to make progress in this regard.

Specifically, clearly defined minimum security criteria have been developed and implemented for the major enrollment sectors, and will be completed for all current enrollment sectors by this summer. The SAFE Port Act requires CBP to work with the COAC to review and modify as appropriate these criteria on an annual basis, and they have done so. This program enhancement will be completed each year as part of the development of the C-TPAT annual plan, another SAFE Port Act requirement. CBP is finalizing revisions to the C-TPAT Strategic Plan, which was first published in December 2004.

The SAFE Port Act also required CBP to review their certification processes for new members, and make adjustments to strengthen this initial review if necessary. They have done so, and all new applications are being reviewed within 90 days.

Additionally, the Act requires that all new certified members undergo their initial validation within 1 year of acceptance into the program, and be revalidated every four years. In 2007, CBP's goal is to complete 3,000 validations. As a point of reference, CBP completed 133 validations in 2003; 287 in 2004; 1,080 in 2005; and 2,398 in 2006. This is real progress, and has been made possible by adding Supply Chain Security Specialists (SCSS) to the program.

With current staffing levels, the C-TPAT program should fulfill its operational goals for both the 2007 and 2008 calendar years. With the projected level of validations and revalidations needed to be in compliance with the Act set at just less than 3,000 per year; the current staff of 150 SCSS's should be able to manage this workload. The SAFE Port Act mandates that all revalidations must occur within 4 years of the initial validation, while the FY07 DHS Appropriations Act called for revalidations to occur within 3 years of the initial validation. Thus, the C-TPAT program is moving forward on a 3 year revalidation model to ensure compliance.

Projected revalidations alone will reach over 2,300 in 2009. The addition of Mexican Highway Carrier validations (done annually due to higher risk models) will add approximately 400. Further, required initial validations within 1 year of certification are being projected at 1,500. As a result, the final validation/revalidation totals needed would well exceed 4,000 for 2009 creating compliance issues with the current staffing numbers.

However, with the identified additional staffing of 50 SCSS's being brought on board sometime in late calendar year 2008, C-TPAT would again see compliance with SAFE Port Act mandated timelines to be well within reach.

CBP has also developed a proposal through discussions with the COAC, where third parties will be used to validate supply chains where CBP currently lacks full

access, and as a result, C-TPAT members are not receiving all the program benefits they are entitled to. Specifically, CBP will pilot using three to four accepted third party validators to perform reviews in China. A solicitation is currently posted to the Federal Business Opportunities website which outlines the requirements and conditions a firm wishing to be selected as a third party validator must meet. Those validation firms selected for this pilot must sign confidentiality agreements, maintain liability insurance, apply for SAFETY Act certification, and remain free from conflict of interests including having any direct or indirect control over the company which is being validated. The pilot program is voluntary, and as outlined in the Act, any C-TPAT member wishing to participate must pay for this service from the validating firm. Those validation firms selected will also be subject to background investigations. The solicitation closes on April 30th, and CBP anticipates that third party validations will begin in China in June.

C-TPAT is an integral part of the CBP multi-layered strategy. CBP works in partnership with the trade community to better secure goods moving through the international supply chain. C-TPAT has enabled CBP to leverage supply chain security overseas where CBP has no regulatory reach. In 2007, CBP will continue to expand and strengthen the C-TPAT program and ensure that certified member companies are fulfilling their commitment to the program by securing their goods moving across the international supply chain to the United States. To carry-out this critical tenet of C-TPAT, teams of SCSS's will conduct validations and begin revalidations of C-TPAT members' supply chains to ensure security protocols are reliable, accurate, and effective.

Pilot integrated scanning system.

Another example of extending port security outward is the Secure Freight Initiative (SFI). SFI is an unprecedented effort to build upon existing port security measures by enhancing the United States government's ability to scan containers for nuclear and radiological materials in seaports worldwide and to better assess the risk of inbound containers.

On December 7, 2006, the Department and the Department of Energy (DOE), in cooperation with the maritime industry and foreign government partners, announced Phase One of the SFI. The lessons learned and experience gained from Phase One represent critical steps in the process of determining whether the concept of 100% overseas scanning is technologically and economically feasible and the degree to which it increases the security of the international supply chain. Phase One will provide lessons and evidence on how this new, integrated suite of radiation detection and radiography technology can meld smoothly into the logistics, operations, and flow of commerce at each different port.

The initial phase of the SFI involves the deployment of a combination of existing technology and nuclear detection devices to three ports as per the requirements of the SAFE Port Act, but will also extend, in limited operation, to three additional

foreign ports. This will provide a more complete analysis for SFI by including different operational and geographic settings at each port. The ports involved include: Port Qasim in Pakistan; Port Cortes in Honduras; Southampton in the United Kingdom; Port Salalah in Oman; Port of Singapore; and the Gamman Terminal at Port Busan in Korea.

Secure Freight will provide carriers of maritime containerized cargo with greater confidence in the security of the shipment they are transporting, and it will increase the likelihood for shippers and terminal operators that the flow of commerce will be both uninterrupted and secure.

This initiative is the culmination of work with other Government agencies, foreign governments, the trade community, and vendors of leading edge technology. The scanning project is a first step toward realizing a greater vision of Secure Freight, a fully integrated global network for risk assessment.

The Department anticipates completing SFI on schedule, and reporting the results as per the requirements of the Act.

International cooperation and coordination.

The Coast Guard has been working with a variety of international organizations including the Asia Pacific Economic Cooperation (APEC) Forum, the Group of Eight (G8), and the Organization of American States (OAS) to conduct capacity building activities to improve the port security regimes of developing countries. Coast Guard representatives serve on maritime security expert groups of these organizations and have been intimately involved in identifying and executing projects.

Of particular note is the Coast Guard work with the OAS, an organization that is specifically mentioned in the SAFE Port Act for close coordination. Through the Inter-American Committee on Counter-Terrorism (an OAS body), and in conjunction with Canada, the Coast Guard is developing a series of exercises and best practice conferences.

Foreign Port Assessments.

The Coast Guard has increased the pace of assessments and is on track to complete an initial assessment of all trading partners by March 2008. The Coast Guard intends to conduct assessments on a two year cycle thereafter.

This two year cycle is consistent with the guidance contained in the FY-07 Appropriations Act, which called on the Coast Guard to double the rate of assessments (basically from three per month to six per month). This reassessment cycle actually exceeds the requirement of the SAFE Port Act which call for reassessments to be conducted on a three year cycle. Additional resources (approx $6.7M which covered the costs of 32 new billets and associated operations and maintenance costs) were provided.

Office of Cargo Security Policy.

The SAFE Port Act established the Office of Cargo Security Policy within the Department of Homeland Security, and required that the Secretary appoint a Director to lead the office. This has been accomplished, with the Director of the Office of Cargo, Maritime, and Trade Policy being the designee.

Research, development, test, and evaluation efforts in furtherance of maritime and cargo security.

The Department of Homeland Security and the Coast Guard have current and planned efforts to support the furtherance of maritime and cargo security. Fifty-seven percent of the Coast Guard Research, Development, Test, and Evaluation (RDT&E) fiscal year 2007 (FY07) project budget supports the furtherance of maritime and cargo security. The Coast Guard RDT&E efforts for FY07 include:

Mission Areas	Programs/Projects
Boarding Team Support and Communications (FY07 funding - $730K)	Maritime Biometrics, ID at Sea Boarding Team Connectivity Next Generation Underway Connectivity Boarding Officer Tools and Equipment Support
Compel Compliance (FY07 funding - $195K)	Anti-Personnel Stopping Mid-Sized Vessels
Platforms and Sensors (FY07 funding - $915K)	Acoustic Buoy Multi-Sensor Performance Prediction Global Observer Small UAS Evaluations
Sector and Port Security Operations (FY07 funding - $389K)	Maritime Domain Awareness Community of Interest National Automatic Identification System
Miscellaneous (FY07 funding - $85K)	Net-Centricity Weapons of Mass Destruction

The Department of Homeland Security Office of Science and Technology (S&T) FY07 funds to the Coast Guard that support the furtherance of maritime and cargo security total $3,687K. The projects include:

Mission Areas	Programs/Projects
Boarding Team Support and Communications (FY07 funding - $1050K)	Boarding Team Communications

Sensor, Data Fusion, & Decision Aids (Maritime) (FY07 funding - $2637K)	Visualization Tools Hawkeye Watch keeper Prototype Offshore Buoys for Vessel Detection Emergence Response Blue Force Tracking Swimmer/Diver Detection Global Observer

S&T FY08 funding has yet to be defined. The Coast Guard is planning a comparable dollar figure to support the furtherance of maritime and cargo security in FY08. Through the S&T-established Capstone Integrated Product Teams (IPT), FY09-FY13 funding has been identified for the furtherance of maritime and cargo security through the Maritime Security Capstone IPT and the Cargo Capstone IPT.

Office of international trade.

The mandates of the SAFE Port Act and the actions of CBP intersected again when CBP formed the Office of International Trade in September 2006. The establishment of this office will serve to strengthen CBP's ability to carry out their mission of facilitating the flow of legitimate trade across U.S. borders while securing the borders and protecting the American economy from unfair trade practices and illicit commercial enterprises. The Office of International Trade consolidates trade policy, program development, and compliance measurement functions into a single office, providing greater consistency within CBP with respect to its international trade programs and operations. In addition, CBP's close working relationship with the trade community, a hallmark of CBP's operations and programs, has been further enhanced. The new Office of International Trade is providing CBP and the Trade community with an organization that can effectively address the growing volume and complexities of international trade and is enabling us to successfully meet the challenges inherent in managing the balance of trade and security.

To meet the Congressional requirements of the SAFE Port Act, CBP is developing a resource optimization model (ROM) for the Office of International Trade. The objectives of the model are to: (1) optimally align the workforce to the Office of International Trade's performance outcomes and goals; (2) adequately staff the priority trade functions; and (3) comply with statutory requirements. The model will be designed to use the new office's performance objectives and goals as inputs to determine the right number and right mix of resources to facilitate legitimate trade.

Additionally, in preparation of submitting a report on the reorganization into the Office of International Trade, CBP has been meeting regularly with the COAC subcommittee on the Office of International Trade. During this first year, the work group will assess improvements to communications as a result of the reorganization, as well as some quantifiable measures for trade facilitation.

Currently, the group is working together to find mutually beneficially process improvements to facilitate legitimate trade, which in turn will assist CBP in its trade enforcement efforts.

Domestic Nuclear Detection Office

The Department of Homeland Security greatly appreciated that Congress formally authorized the Domestic Nuclear Detection Office (DNDO) in the SAFE Port Act. Recently celebrating its second anniversary, DNDO is a vital component in the Departments ability to develop and implement WMD detection and response capabilities.

Conclusion

The steps the Department of Homeland Security is taking to implement the SAFE Port Act are and will be an extremely important aspect to the security of the nation's port facilities and vessels. Through the SAFE Port Act, Congress has recognized and bolstered many of our aggressive programs to protect our ports. We appreciate the close cooperative relationship the Department and its component agencies had with the House and Senate in the development of the Act, and look forward to the continued interaction to promote our mission and ensure the safety of American citizens and commerce.