



# Department of Homeland Security Office of Inspector General

## DHS' Plan for Implementing Secure Systems of Transportation



*Office of Inspector General*

**U.S. Department of Homeland Security**  
Washington, DC 20528



**Homeland  
Security**

October 24, 2008

### Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

This report addresses the status of DHS' plan to secure systems of transportation as required by the *Coast Guard and Maritime Transportation Act of 2004*. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner  
Inspector General

# Table of Contents/Abbreviations

---

Executive Summary .....	1
Background.....	2
Results of Audit .....	3
Implementation Status of the Plan as of May 31, 2008.....	3
Late Submission of Plan to Congress .....	6

## Appendices

Appendix A: Purpose, Scope, and Methodology.....	8
Appendix B: Management Comments.....	9
Appendix C: Status of Programs and Systems from the DHS Plan .....	11
Appendix D: National Planning Structure as Related to the International Cargo Supply Chain .....	23
Appendix E: Major Contributors to This Report.....	24
Appendix F: Report Distribution .....	25

## Abbreviations

ACE	Automated Commercial Environment
ATS	Automated Targeting System
CBP	Customs and Border Protection
CONOPS	Concept of Operations
C-TPAT	Customs-Trade Partnership Against Terrorism
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
GAO	Government Accountability Office
MTSA	Maritime Transportation Security Act of 2002
NORM	naturally occurring radioactive material
OIG	Office of Inspector General
PEP	Project Execution Plan
PVT	polyvinyl toluene
SFI	Secure Freight Initiative

# OIG

---

*Department of Homeland Security  
Office of Inspector General*

## **Executive Summary**

Pursuant to the *Coast Guard and Maritime Transportation Act of 2004*, the Department of Homeland Security must submit to Congress a plan for implementing secure systems of transportation by February 2005. The Act also required DHS to: analyze the resources necessary to conduct validations of trade partners; track containers entering the United States; develop international standards; and collect user fees. The Coast Guard Act also required us to report on the progress made by the department in implementing the plan.

The department issued its *Report to Congress on Secure Systems of Transportation* on September 6, 2007, 2 1/2 years after the due date. By this time, the plan had been superseded by the passage of the *Security and Accountability for Every Port Act of 2006*. Although broader in scope, the *Security and Accountability for Every Port Act of 2006* repeated and clarified the requirements of the Coast Guard Act. Although the department issued the plan late, it proceeded with the implementation of the programs and systems to secure systems of transportation. Also, the department did not timely conduct the analyses required by the Coast Guard Act. This report provides the status of the 10 programs and systems listed in the plan as of May 31, 2008.

Appendix D charts the relationships among the different requirements and the department's plans on supply chain security.

Due to the actions taken by the Secretary to ensure timely responses to congressional requests, we are not making recommendations in this report. Comments from Department of Homeland Security management are included in appendix B.

---

## Background

In response to the events of September 11, 2001, Congress passed the *Maritime Transportation Security Act of 2002* (MTSA) to protect America's maritime community against the threat of terrorism without adversely affecting the flow of U.S. commerce. One provision of MTSA required a program to evaluate and certify secure systems of international intermodal transportation. DHS assumed responsibility for MTSA after the Coast Guard transitioned to DHS in April 2003, pursuant to requirements of the *Homeland Security Act*.

*The Coast Guard and Maritime Transportation Act of 2004* required DHS to submit a plan to implement the program required by MTSA by February 2005. The Act also required the DHS Office of Inspector General (OIG) to report on DHS' progress in implementing the plan. DHS' Border and Transportation Security Directorate was responsible for preparing the plan, but the DHS Secretary abolished the directorate as part of an initiative to streamline DHS' organizational structure. The Office of Policy assumed responsibility for coordinating plan development.

Although broader in scope, the *Security and Accountability for Every Port Act of 2006* (the SAFE Port Act) repeated and clarified requirements of both MTSA and the Coast Guard Act. The SAFE Port Act addressed security matters related to the movement of containers through the international supply chain. The Act created and codified new programs and initiatives, and amended some of the original provisions of MTSA. It included provisions that codified the Container Security Initiative and the Customs-Trade Partnership Against Terrorism (C-TPAT)—two programs administered by Customs and Border Protection (CBP) to help reduce threats associated with cargo shipped in containers. The Act also established the Domestic Nuclear Detection Office (DNDO) to complete a global nuclear detection architecture.

Further, the SAFE Port Act created an Office of Cargo Security Policy within DHS Office of Policy and tasked this office to coordinate all DHS policies relating to cargo security and to work with stakeholders and other federal agencies to establish standards and regulations and to promote best practices. The SAFE Port Act also required DHS to develop a strategic plan to enhance international supply chain security. DHS fulfilled this requirement in July 2007 by issuing the *Strategy to Enhance International Supply Chain Security*. In October 2007, the Government Accountability Office (GAO) testified before Congress on DHS' progress in implementing the SAFE Port Act. The testimony highlighted improvements and challenges that DHS faces in three areas: overall port security, port facility security, and container security.

---

## Results of Audit

### Implementation Status of the Plan as of May 31, 2008

In September 2007, DHS issued the *Report to Congress on Secure Systems of Transportation*—its plan for implementing secure systems of transportation in response to requirements of the Coast Guard Act. The plan provides information on implementation of various programs and systems to secure systems of transportation, but does not include the specific analyses required by the Coast Guard Act.

#### Status of Programs and Systems in the Plan

The following is a brief overview and status update regarding the 10 programs and systems the department instituted to help secure maritime containers entering the United States.

- **The Customs-Trade Partnership Against Terrorism (C-TPAT)** is a voluntary government-business initiative designed to improve international supply chain security by providing incentives to businesses that meet certain security standards. As of May 31, 2008, CBP had certified 8,455 importers, carriers, and brokers as C-TPAT partners. The SAFE Port Act requires CBP to certify members within 90 days, to validate those companies certified within 1 year of certification, and to conduct revalidations every 4 years to the extent possible and practical. As of May 31, 2008, CBP had 10 applicants for C-TPAT certification that were outstanding for more than 60 days and 2 that were outstanding for more than 90 days.
- **The Container Security Initiative** is a program in which CBP works with foreign customs organizations to shift the screening of maritime containerized cargo destined for the United States from domestic ports of entry to foreign ports of lading. As of May 31, 2008, CBP had met its goal of implementing the Container Security Initiative at 58 ports worldwide to prescreen 85 % of maritime containerized cargo destined for the United States.
- **The Automated Targeting System (ATS)** is a decision support system that performs an automatic risk assessment of cargo using weighted rules and measures. ATS alerts CBP officers of cargo that meets or exceeds predefined criteria. CBP continuously works to improve ATS with new technologies, techniques, and data sources. As of May 31, 2008, CBP met its goal of screening 100 % of inbound cargo containers through ATS. Screening is defined as a visual or automated review of information about goods to determine the

---

presence of improperly declared, restricted, or prohibited items and to assess the level of threat posed by such cargo.

- **The Automated Commercial Environment (ACE)** is a system that allows CBP and the trade community to submit and retrieve data electronically through a secure Web portal. ACE will modernize targeting, inspection, enforcement, revenue collection, and trade statistics processing. CBP began developing ACE in August 2001 and plans to complete development by 2012. As of May 31, 2008, five ACE processes were operational, including: electronic truck manifest, cargo admissibility, cargo examination, cargo release, and conveyance crossing history.
- **The Secure Freight Initiative (SFI)** is a pilot program at foreign ports for testing the feasibility of scanning 100 % of U.S.-bound containerized cargo with radiation detection equipment and nonintrusive imaging equipment. As of May 31, 2008, CBP was expanding SFI to additional foreign ports to test other challenges to the 100 % scanning goal. In June 2008, CBP reported to Congress on the legal, logistical, and technical challenges facing SFI.
- **The World Customs Organization** is an intergovernmental organization that developed the voluntary international customs standards known as the World Customs Organization SAFE Framework of Standards. As of May 31, 2008, 152 of 173 organization members, including the United States, had signed a letter of intent to implement the SAFE Framework of Standards. Domestically, CBP is on step five of the six-step implementation process.
- **The International Ship and Port Facility Security Code** is an amendment to the International Maritime Organization's International Convention for the Safety of Life at Sea. This code prescribes minimum-security requirements to detect security threats and to take preventive measures against security incidents affecting ships and port facilities used in international trade. The DHS Secretary is required to assess the effectiveness of the antiterrorism measures maintained at foreign ports from which foreign vessels depart for the United States. As of May 31, 2008, the Coast Guard continues to conduct foreign port visits on a 2-year cycle.
- **Maritime Domain Awareness** is the understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States. The breadth of Maritime Domain Awareness requires a unified effort

---

through a collaborative network of partners. The National Concept of Operations for Maritime Domain Awareness lists various short-term goals for 0 to 5 years, midterm goals for 6 to 10 years, and long-term goals for 11 to 20 years. As of May 31, 2008, the Coast Guard had established the Maritime Domain Awareness Stakeholder Board to provide a cohesive governance structure for interagency efforts.

- **The Advanced Spectroscopic Portal** is a next-generation passive detection radiation portal monitor using spectroscopic analysis to distinguish between special nuclear materials and naturally occurring nuclear materials. As of May 31, 2008, DNDO was conducting performance tests to validate the Advanced Spectroscopic Portal's detection abilities.
- **The Cargo Advanced Automated Radiography System** is a next-generation nonintrusive imaging system jointly managed by DNDO and CBP to improve CBP's ability to identify shielded special nuclear materials. DNDO plans to complete developmental tests and evaluations of the system's prototypes and a cost-benefit analysis of the entire program. As of May 31, 2008, the Cargo Advanced Automated Radiography System was in development and testing.

For more detailed discussion of each program or system, including the status of open recommendations from previous GAO and OIG audits, see appendix C.

### **Status of Analyses Required by Congress**

By 2006, DHS had not submitted to Congress the four analyses that the Coast Guard Act required. Congress repeated three of these requirements in greater detail in the SAFE Port Act of 2006. Following is the status of the three analyses required by the Coast Guard Act and repeated in the SAFE Port Act:

- Section 218(a) required DHS to develop a plan to implement a 1-year voluntary pilot program to test and assess the feasibility, costs, and benefits of using third-party entities to conduct validations of C-TPAT participants. Section 218(b) required DHS to submit a report to Congress on the plan. On May 8, 2007, DHS transmitted the *Report to Congress on SAFE Port Act Section 218(b): Customs-Trade Partnership Against Terrorism (C-TPAT) Third Party Validators Pilot Program Plan*.
- Section 406 required DHS to submit a report to Congress on in-bond cargo, including a plan for tracking in-bond cargo within the



---

Automated Commercial Environment. On October 17, 2007, DHS transmitted the *Report to Congress on In-Bond Cargo*.

- Section 204(c) encouraged the DHS Secretary to promote and establish international standards for the security of containers moving through the international supply chain with foreign governments and international organizations. On May 18, 2007, DHS sent a letter to Congress explaining its decision not to initiate a rulemaking proceeding to establish minimum standards for securing containers in transit to the United States. In lieu of establishing standards, DHS requires C-TPAT participants to affix a high-security seal that must meet or exceed current international standards to all loaded containers bound for the United States.

The fourth analysis required by the Coast Guard Act was repeated in the *Implementing Recommendations of the 9/11 Commission Act of 2007* (the 9/11 Act). The 9/11 Act required DHS to conduct a study of the need for and feasibility of establishing a system of maritime and surface transportation-related user fees that may be imposed and collected as a dedicated revenue source. As of October 2008, the department was reviewing a draft of the study on user fees.

## **Late Submission of Plan to Congress**

DHS issued its plan for implementing secure systems of transportation on September 6, 2007—2 1/2 years late. The Coast Guard Act required DHS to submit the plan to Congress within 180 days of enactment, which was February 7, 2005.

The plan was developed to serve a twofold purpose. The *Intelligence Reform and Terrorism Prevention Act of 2004* required DHS to submit to Congress a report of the status of MTSA's program to evaluate and certify systems of transportation by March 17, 2005. Both the DHS plan and this new statutory requirement dealt with the same program, so DHS decided to merge the two requirements into one document.

Initially, the Border and Transportation Security directorate convened a group of subject matter experts from across DHS to prepare the plan. After the DHS Secretary abolished that directorate as part of an initiative to streamline DHS' organization structure, the Office of Policy, which was established in July 2005, took over coordination of plan development. DHS then spent 5 months reviewing the plan and later spent 4 months responding to the Office of Management and Budget's comments on it. Another 7 months elapsed between the Office of Management and Budget's clearance of the plan and its issuance.

---

In 2005, the new DHS Secretary made meeting congressional requests a higher priority because of the large number of inquiries that had not yet been responded to and the difficulties in providing timely responses. The department issued a management directive to improve DHS' responsiveness to congressional requests. The directive provides clear guidance on the roles and responsibilities of various DHS officials and their offices in reviewing and addressing congressional requests.

In addition, DHS developed a tracking system to help meet its congressional requirements. Each week, the system is updated and shared with the Secretary's Office. DHS also sends weekly reminders to component points of contact asking them to examine requests and update the system on progress or any delays in responding to them. Due to the actions taken by the Secretary to ensure timely responses to congressional requests, we are not making recommendations in this report.

## **Appendix A**

### **Purpose, Scope, and Methodology**

---

The *Coast Guard and Maritime Transportation Act of 2004* required DHS to submit a plan to Congress for implementing secure systems of transportation. The Act also required us to report on the department's progress in implementing the plan. The objective of our audit was to determine DHS' progress in implementing its plan for securing systems of transportation.

We performed our audit fieldwork in Washington, D.C. Within DHS, we visited the Office of Policy, the Office of General Counsel, the Office of Chief Financial Officer, CBP, the Coast Guard, and DNDO. In addition, we contacted officials from the Operations Coordination and Planning Directorate.

We worked with the DHS Office of General Counsel and the Cargo, Maritime and Trade unit of the Office of Policy Development to determine how DHS met the Coast Guard Act requirements by addressing subsequent legislative requirements. Also, we reviewed how DHS offices and bureaus implemented the plan.

In addition, we reviewed the 10 programs and systems listed in the plan to determine how they will help to secure systems of international intermodal transportation, their status as of May 31, 2008, and the status of prior audit recommendations. We reviewed strategic plans, implementation plans, performance measures, reports to Congress, prior audit reports, and other documentation for each of the 10 programs and systems. Our discussion of the status of the 10 programs and systems contains information from both published reports and unaudited DHS management assertions.

We reviewed the internal controls DHS put in place to meet congressional mandates. We interviewed DHS Office of General Counsel and Office of Chief Financial Officer officials involved in the process. We examined samples of the tracking system and reviewed the DHS management directive addressing the review and coordination of legislative documents.

We conducted our audit between April and July 2008, according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. Our reporting of the status of programs from the DHS Plan as of May 31, 2008, includes unaudited DHS management assertions. We believe that the evidence obtained, except as noted above, provides a reasonable basis for our findings and conclusions based on our audit objective.

## Appendix B Management Comments

---

U.S. Department of Homeland Security  
Washington, DC 20528



Homeland  
Security

AUG 28 2008

Mr. Richard Skinner  
Inspector General  
Office of Inspector General  
U.S. Department of Homeland Security  
Washington, D.C. 20528

Dear Mr. Skinner:

Thank you for providing us with a copy of the draft report entitled "DHS Plan for Implementing Secure Systems of Transportation" that examines how the Department of Homeland Security (DHS) fulfilled requirements of the *Coast Guard and Maritime Authorization Act of 2004* (Coast Guard Act). The Office of Inspector General (OIG) report notes the late submission of the *Report to Congress on Secure Systems of Transportation* (known as the Plan). It also fairly recognizes the substantially duplicative requirement in Section 201 of the *Security and Accountability for Every Port Act of 2006* (SAFE Port Act) to produce a strategy on the same topic required in the Plan, and that this strategy was timely submitted to Congress.

DHS concurs with the OIG's finding that the required Plan was not submitted to Congress until September 6, 2007. However, as you noted in your report, the development of the Plan was undertaken during a period of significant transition within DHS. The development of the report was initially delegated to the Border and Transportation Security Directorate (BTS). During its existence, BTS handled both policy and operational functions, including direct oversight over the DHS components with the operational duties for the requirements of the Coast Guard Act. BTS was eliminated in 2005 during the Second Stage Review, providing the operational components direct reporting authority to the Secretary and establishing the Office of Policy. The Office of Policy became the primary policy division of DHS with policy formulation functions and coordinating responsibilities for the Department's initiatives and programs. Additionally, a new Office of Cargo Security Policy was created within DHS Policy by the *SAFE Port Act*. This office does not retain any operational responsibilities, and instead serves as the primary policy formulation and coordination entity for cargo issues within DHS. The transition from dual operational and policy functions to an exclusively policy component resulted in a new Office of Cargo Security Policy that was less suited to complete the implementation aspect of the Coast Guard Act requirements, further resulting in a time lag as components were engaged.

I would also like to note that your report fairly acknowledges that while the required plan was submitted late to Congress, we have continued throughout the entire time period to implement and operate the programs and policies that actually secure systems of transportation. The programs discussed in your report, such as the Customs Trade Partnership Against Terrorism, the

[www.dhs.gov](http://www.dhs.gov)

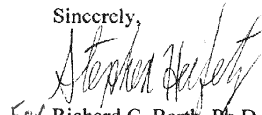
**Appendix B**  
**Management Comments**

---

Container Security Initiative, the Secure Freight Initiative, the Automated Targeting System, and Maritime Domain Awareness, have contributed significantly to the progress DHS has made toward securing America's ports-of-entry, facilitating legitimate trade and travel, and ensuring the vitality of our economy.

We thank you again for the opportunity to review this report and to provide comments.

Sincerely,



For Richard C. Barth, Ph.D.  
Assistant Secretary for Policy Development  
Department of Homeland Security

## **Appendix C**

### **Status of Programs and Systems from the DHS Plan**

(The Status as of May 31, 2008 includes unaudited DHS management assertions.)

---

#### **Customs-Trade Partnership Against Terrorism (C-TPAT)**

C-TPAT is a voluntary government-business initiative to build cooperative relationships that strengthen and improve overall international supply chain and U.S. border security. Its goal is to shift responsibility for cargo security onto stakeholders in the supply chain. C-TPAT companies commit to meeting security standards in order to use their leverage to prevent terrorist organizations from exploiting their supply chains, thereby reducing the risk that a terrorist weapon will be introduced into, or concealed within, one of their shipments. Central to the security vision of C-TPAT is the core principle of increased facilitation for legitimate business entities that are compliant traders. In exchange for meeting minimum-security standards, cargo of C-TPAT partners is subject to fewer inspections upon arrival, thereby making C-TPAT-secured shipments move faster and more predictably.

CBP conducts domestic and foreign site visits to physically review companies and to identify both weaknesses and best practices within their supply chains. C-TPAT has enabled CBP to leverage supply chain security throughout international locations where CBP has no regulatory reach. Further, CBP plans to internationalize the C-TPAT core principles through cooperation and coordination with the international community. C-TPAT is currently pursuing mutual recognition arrangements with several foreign partnership programs.

CBP's goal is to screen and separate transactions involving known low-risk trade from the unknown high-risk trade. Ultimately, if C-TPAT partners adopt supply chain security best practices, the risk that terrorists could exploit their shipments to the United States will be reduced. This will allow CBP to focus efforts on higher risk shipments.

The SAFE Port Act of 2006 codified C-TPAT and requires C-TPAT to monitor the timeframes established to complete certain objectives. The 2008 C-TPAT Annual Plan includes new performance measures to ensure compliance with these requirements. The 2007–2012 C-TPAT Strategic Plan specifies the goals and objectives for C-TPAT and is aligned with and supports CBP's Strategic Plan for Preventing Terrorist Weapons from Entering the United States.

As of May 31, 2008, CBP has certified 8,455 importers, carriers, and brokers as C-TPAT partners and completed 8,056 validations. There have been 556 suspensions or removals. CBP averages 145 validations per month and has 200 positions assigned to C-TPAT.

## **Appendix C**

### **Status of Programs and Systems from the DHS Plan**

---

From 2003 through 2008, GAO conducted three audits of C-TPAT. These audits made 14 recommendations, of which 6 were open as of May 31, 2008. Of the open recommendations, five are from a GAO report issued in April 2008. The open issues relate to improving performance measures, improving the validation process, and adding data elements to the records management system.

#### **Container Security Initiative**

As a critical element of DHS' multilayered defense strategy, the Container Security Initiative supports the CBP priority mission, which is to prevent terrorists and terrorist weapons from entering the United States, while facilitating and maintaining legitimate trade. The Container Security Initiative has shifted the screening process of containerized maritime cargo to an earlier stage in the international maritime supply chain, from the domestic ports of entry to the foreign ports of lading. Under the initiative, CBP deploys a multidisciplinary team of DHS officers to work with the host nation to target containerized maritime cargo that may pose a risk of terrorism and to screen containers before they are loaded on vessels destined for the United States. DHS officials work with host country counterparts to share information and establish security criteria for identifying high-risk containers. Foreign customs administrations use standard protocols and nonintrusive technologies to examine mutually designated high-risk maritime containers before they are shipped to U.S. ports. As of May 31, 2008, no implements of terrorism have been detected in maritime containerized cargo destined for the United States.

As of May 31, 2008, CBP has met its goal to implement the initiative at 58 total ports worldwide to prescreen 85 % of maritime containerized cargo destined to the United States. Since CBP met this goal on September 28, 2007, there are no plans to expand the initiative. CBP works closely with the World Customs Organization, the European Union, and the G-8 countries to adopt standards similar to the Container Security Initiative and recommend these standards to their members. Currently, CBP is exploring remote targeting, coupled with the use of real-time remote imaging of container examinations incorporating a live video feed, to monitor the inspection process at the National Targeting Center-Cargo. CBP is testing performance measures from the Container Security Initiative Strategic Plan for 2006–2011 at various ports. The measures may be revised based on the pilot evaluation. Targets will be established once the measures have been solidified.

Originally, another goal of the initiative was to equip containers with security devices that would communicate evidence of seal tampering. The container security devices would register every opening, whether

## **Appendix C**

### **Status of Programs and Systems from the DHS Plan**

---

legitimate or unauthorized. In a May 2007 letter to Congress, DHS stated that although the technology for the desired container security devices did not exist, DHS was working with industry to develop it.

From 2003 through 2008, GAO conducted three audits of Container Security Initiative. These audits made nine recommendations, of which three were open as of May 31, 2008. The open issues relate to improving performance measures, strengthening CBP's process for evaluating initiative teams at overseas ports, and improving information gathered about host governments' examination systems.

#### **Automated Targeting System (ATS)**

CBP has integrated ATS into its multilayered approach to security by using it as a tool for researching and targeting high-risk cargo for further review or examination. CBP uses ATS as a decision support tool for CBP officers working at U.S. ports of entry and at Container Security Initiative ports overseas. ATS performs an automated risk assessment of cargo information using weighted rules to determine the relative risks. Through these rules, ATS alerts the CBP officers to shipments that meet or exceed predefined criteria. In addition, ATS can detect significant anomalies by electronically matching manifest and entry data to Dun & Bradstreet records, law enforcement records, and enforcement data provided by other government agencies.

CBP continuously works to improve the targeting system with new technologies, techniques, and data sources. This is necessary because of constantly shifting threats and the diversity of international trade. CBP has been exploring advanced analytical tools to assess the incorporation of additional smart features into ATS. For example, CBP has projects under development to implement predictive modeling, anomaly detection, and visualization tools that are customized to analyze cargo shipments in ATS.

As of May 31, 2008, CBP has completed many ATS initiatives to target high-risk cargo. A key performance measure for ATS is screening 100 % of inbound cargo containers. Screening is defined as a visual or automated review of information about goods to determine the presence of improperly declared, restricted, or prohibited items and to assess the level of threat posed by such cargo. Other performance measures include number of shipments, shipments held, percent mitigated, and shipments designated intensive.

From 2003 through 2008, GAO conducted two audits of ATS and DHS OIG conducted four. These audits made 25 recommendations, of which 3 were open as of May 31, 2008. The open issues relate to improving



## **Appendix C**

### **Status of Programs and Systems from the DHS Plan**

---

documentation of examinations, testing, and threat assessments. Currently, the OIG is conducting an audit of ATS.

#### **Automated Commercial Environment (ACE)**

Congress funded ACE in response to the trade community's concerns that federal requirements were outdated, burdensome, and duplicative. The ACE system will modernize the targeting, inspection, enforcement, revenue collection, and trade statistics processes for all cargo entering and leaving the United States. CBP is responsible for enforcing U.S. trade laws while simultaneously facilitating legitimate international trade. One of CBP's critical functions is to control cargo and conveyances entering and leaving the United States to prevent smuggling of instruments of terrorism, narcotics, and illegal aliens, as well as to enforce trade laws and collect revenue. CBP's ability to process the growing volume of imports, while improving compliance with trade laws and border security, depends heavily on improving the trade compliance process and modernizing supporting automated systems.

CBP began developing ACE in August 2001 and plans to complete development by 2012. Once fully implemented, ACE will enable the trade community and CBP officers to submit and retrieve import transaction data electronically through an intuitive, standards-based, secure Web portal. The ACE Program Plan has a series of target dates for all the processes leading to the completion of the system in 2012. The Critical Path Method allows CBP to track the dates and identify whether goals are late and what effect delays may have on the milestone dates. CBP internally tracks the 15 performance measures listed in the quarterly report to Congress to monitor ACE's progress.

ACE will support border security by enhancing analysis and information sharing with other government agencies. ACE will also provide CBP with the means to decide, before a shipment reaches the border, whether the shipment should be targeted as a security threat or should be expedited because it complies with U.S. laws. ACE will accomplish this by consolidating rail and sea shipment manifest and entry data to help identify risky shipments; providing a three-dimensional view of conveyance stowage plans to help identify unmanifested containers; allowing CBP officers to place or remove holds at the container level; providing CBP officers with integrated entry, manifest, and risk assessment information for informed cargo processing decisions; and streamlining the process for placing or removing holds by other government agencies. ACE will provide a "single window" for submitting trade information to federal agencies that share responsibility for facilitating international trade and securing the U.S. supply chain.

## **Appendix C**

### **Status of Programs and Systems from the DHS Plan**

---

As of May 31, 2008, five high-level ACE processes designed to gather cargo information were operational. Performed in concert with ATS, these processes provide additional information on electronic truck manifests, cargo admissibility, assists in better targeting of cargo, controlling and improving cargo release, and provides conveyance crossing history. Of the 44 federal agencies that will participate in ACE, 25 already have access to ACE, with a total of 375 users.

From 2003 through 2008, GAO conducted four audits of ACE and DHS OIG conducted six. These audits made 34 recommendations, of which 13 were open as of June 2008. The open issues relate to implementing an accountability framework, minimizing overlap across ACE releases, improving risk management, improving reporting, developing policies and procedures to improve management, and improving security.

#### **Secure Freight Initiative (SFI)**

CBP is responsible for preventing weapons of mass destruction from entering the United States in cargo containers that are shipped from more than 700 foreign seaports. The SAFE Port Act calls for testing the feasibility of scanning 100 % of U.S.-bound cargo containers using nonintrusive imaging equipment and radiation detection equipment at foreign seaports. The 9/11 Act requires scanning 100 % of U.S.-bound cargo containers by 2012. SFI began as a pilot program at three foreign ports (Port of Southampton, U.K.; Port Qasim, Pakistan; and Puerto Cortez, Honduras) to test the feasibility of scanning 100 % of U.S.-bound containerized cargo.

CBP's report and testimony to Congress in June 2008 concluded that the initial SFI deployments indicate that scanning U.S.-bound maritime containers is possible on a limited scale. However, SFI operations in these initial locations benefited from considerable host nation cooperation, low transshipment rates, and technology and infrastructure costs covered primarily by the U.S. government. The total U.S.-bound container volume at these three ports from October 12, 2007, to May 25, 2008, was 170,564 containers. Every year, 11.5 million maritime containers enter the United States.

The deployment of container-scanning equipment at each of the SFI ports has presented certain operational, technical, logistical, financial, and diplomatic challenges that will likely continue to be encountered as SFI deploys to additional locations. One challenge has proven particularly difficult to overcome: operating these systems in a transshipment port. Transshipment is where containers arrive on one ship and depart on

## **Appendix C**

### **Status of Programs and Systems from the DHS Plan**

---

another without entering or exiting through the port gates. The initial SFI pilots have demonstrated that technical and operational solutions are not yet available to capture transshipped cargo efficiently. Further, technological improvements to next-generation radiation detection and imaging equipment will be needed to implement the SFI program efficiently and effectively.

As of May 31, 2008, CBP was expanding SFI to include three additional foreign ports (the Modern Terminal in Hong Kong; the Port of Salalah, Oman; and the Gamman Terminal in Busan, South Korea) on a limited basis to test other challenges to the 100 % scanning goal. CBP chose these ports because they present a unique set of challenges and provide diverse environments in which to evaluate different options.

In June 2008, CBP reported to Congress on the legal, logistical, and technical challenges facing SFI. Also in June 2008, GAO testified on the challenges related to continuing SFI: workforce planning, host nation examination practice, performance measurement, resource responsibilities, logistics, technology and infrastructure, use and ownership of data, consistency with risk management, and reciprocity and trade concerns. In addition, GAO started a comprehensive audit of the SFI Pilot Program in July 2008.

#### **World Customs Organization SAFE Framework of Standards**

The World Customs Organization, a global intergovernmental organization, represents 173 customs administrations responsible for processing more than 98 % of all international trade. In 2005, members developed a set of voluntary international customs standards, known as the World Customs Organization SAFE Framework of Standards, to enhance the security of the supply chain and facilitate international trade. In June 2005, CBP was one of the first international customs organizations to submit a Letter of Intent to adopt the SAFE Framework. Full implementation of the SAFE Framework entails adoption by all members.

The SAFE Framework aims to establish customs-to-customs network arrangements that will strengthen cooperation among customs administrations, enabling them to carry out controls earlier in the supply chain. For example, the administration of an importing country can request the administration of the exporting country to conduct an examination on its behalf. Capacity building and mutual recognition arrangement are two core components of World Customs Organization activity. The organization has to be flexible to help other countries to implement the SAFE framework requirements according to their level of development, while at the same time ensuring safe transportation of cargo

## **Appendix C**

### **Status of Programs and Systems from the DHS Plan**

---

to the United States. The Capacity Building Operational Strategy program seeks to deliver the customs services required to support economic development in all members. The mutual recognition arrangement is a nonbinding document that allows members of one program to receive comparable benefits in the other program. Mutual recognition of customs-to-business partnership arrangements will benefit both industry and government.

As of May 31, 2008, 152 of 173 World Customs Organization members had signed the Letter of Intent to implement the SAFE Framework of Standards to Secure and Facilitate Global Trade. Also, more than 60 administrations have entered the implementation phase. The United States has not fully implemented the SAFE Framework; CBP is on step five of the six-step process. In addition, the United States is supporting 10 partner nations in implementing diagnostic tools for surveying port and trade security.

#### **International Ship and Port Facility Security Code**

The International Ship and Port Facility Security Code is an amendment to the United Nations International Maritime Organization's International Convention for the Safety of Life at Sea. The code prescribes minimum-security requirements for governments, shipping companies, shipboard personnel, and port and facility personnel to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade. The DHS Secretary is required to assess the effectiveness of the antiterrorism measures maintained at foreign ports from which foreign vessels depart to the United States.

The Coast Guard, through the International Port Security Program, encourages multilateral discussions with nations to exchange information and best practices. This program aligns MTSA's implementation and enforcement requirements with the International Ship and Port Facility Security Code and other international maritime security standards. This alignment directly supports the National Strategy for Maritime Security and the National Plan to Achieve Maritime Domain Awareness. The International Port Security Program further supports the Coast Guard's effort to safeguard the international transportation system by working closely with international trading partners to promote reasonable and consistent implementation of the code.

The International Port Security Program's strategic goal is to reduce risk to the national maritime transportation system by working with foreign maritime trading partners to strengthen antiterrorism measures in overseas ports. The Coast Guard plans to set conditions for entry of vessels arriving from ports with inadequate antiterrorism measures, improve port

## **Appendix C**

### **Status of Programs and Systems from the DHS Plan**

---

security capacity, and improve maritime governance both domestically and abroad. The Coast Guard also plans to visit all trading partner nations at least once a year, with a more formal visit at least every other year. Country visits will be scheduled based on a variety of factors, including the prioritized country list, Headquarters' programmatic and policy concerns, the Area Commander's priorities and concerns, results of prior visits, political considerations, and a country's receptivity to receiving a visit. When the Coast Guard finds that a country's antiterrorism measures are inadequate, the Coast Guard imposes conditions of entry on vessels from that country's ports to mitigate the risk to the United States. To date, the Coast Guard has imposed conditions of entry on nine countries.

As of May 31, 2008, International Port Security Program managers stated that the budget was adequate based on the current resources and personnel available to conduct visits. The program has 63 positions assigned. In accordance with the *Department of Homeland Security Appropriations Act, 2007*, program management expects to continue to conduct foreign port visits on a 2-year recurring cycle. The Coast Guard has completed the first round of visits in more than 140 countries and has commenced the second round of visits.

#### **Maritime Domain Awareness**

Maritime Domain Awareness is the understanding of anything associated with the global maritime domain that could affect the security, safety, economy, or environment of the United States. It is a key component of an active, layered maritime defense that supports the President's National Strategy for Maritime Security. No one country, department, or agency can achieve effective awareness; only through unity of effort can the security, safety, economic, and environmental objectives associated with Maritime Domain Awareness be achieved.

Maritime Domain Awareness will help to safeguard U.S. systems of transportation when legacy information and intelligence systems are integrated with current and emerging intelligence capabilities. This integration will fuse information into a common operational picture available to maritime operational commanders and accessible throughout the global maritime community of interest. The Coast Guard was the primary DHS lead in creating and developing the National Strategy, the National Plan to Achieve Maritime Domain Awareness, and the National Concept of Operations (CONOPS) for Maritime Domain Awareness. This National Concept of Operations lists various short-term goals for 0 to 5 years, midterm goals for 6 to 10 years, and long-term goals for 11 to 20 years.

## **Appendix C**

### **Status of Programs and Systems from the DHS Plan**

---

Recognizing that numerous existing facilities already contribute to Maritime Domain Awareness, the National CONOPS established the Stakeholder Board to lead the overall national effort and designated Enterprise Hubs to coordinate information flow for the respective subject areas. Enterprise Hubs are existing organizations within DHS and the Department of Defense that already possess subject matter expertise, a preponderance of the requisite authorities, and knowledge of associated capabilities and procedures. Employing these coordinated information collection and sharing capabilities will maximize near-real time awareness of maritime threats. The CONOPS established an interagency leadership structure to coordinate and unify efforts. The governance structure consists of a Stakeholder Board co-chaired by the directors from the Global Maritime Intelligence Integration board and the Global Maritime Situational Awareness board.

Maritime Domain Awareness can be achieved by improving U.S. ability to collect, fuse, analyze, display, and disseminate actionable information and intelligence to operational commanders. This plan advocates enhanced and innovative collection of intelligence, the integration of correlated open source information, and the incorporation of automated algorithms to assist human analytic efforts. The primary method for information sharing, situational awareness, and collaborative planning will be a national maritime common operational picture. This picture will provide a uniform source and display of data that is transferred to a near-real time, virtual information grid to be shared by all federal, state, and local agencies with maritime interests and responsibilities—except when limited by security, policy, or regulations. Within the next few years, a user-defined operational picture will be implemented.

Establishing the Stakeholder Board in December 2007 was the first step in meeting the numerous near- and long-term goals set by the National Plan to Achieve Maritime Domain Awareness and the National CONOPS. At one time, the Coast Guard Maritime Domain Awareness staff responsible for Coast Guard's input into these documents included 30 personnel. However, its numbers have since been reduced to fewer than five full-time employees as duties have been picked up by the Stakeholder Board and other Coast Guard divisions.

GAO is currently preparing an audit report for its audit of Coast Guard efforts to achieve Maritime Domain Awareness.

#### **Advanced Spectroscopic Portal Program**

DNDO's mission is to complete a global nuclear detection architecture that includes developing nuclear and radiation detection technologies. One such technology is the Advanced Spectroscopic Portal, a next-

## **Appendix C**

### **Status of Programs and Systems from the DHS Plan**

---

generation passive detection radiation portal monitor using spectroscopic analysis to distinguish between special nuclear materials used to construct nuclear weapons (such as highly enriched uranium) and naturally occurring radioactive material (NORM). The joint DNDO-CBP program seeks to design, acquire, and test Advanced Spectroscopic Portals and to deploy them at CBP ports of entry as part of a multilayered system of radiation detection.

Ultimately, DNDO hopes that the Advanced Spectroscopic Portal program will improve radiological and nuclear detection and identification while minimizing impact on legitimate commerce. Currently, CBP's standard scanning procedure begins with a primary screen in which CBP officers pass the cargo through polyvinyl toluene (PVT) radiation portal monitors. However, PVT cannot distinguish between different radiological isotopes. Both special nuclear materials and NORMs such as granite, ceramics, and cat litter can trigger a radioactivity alert. If the alarm sounds, CBP officers conduct a secondary inspection. These secondary inspections take approximately 15 minutes to complete. The Port of Los Angeles had 500 to 600 false alarms per day in which the secondary inspection determined that the radioactive material was a NORM. The Advanced Spectroscopic Portal's potential to differentiate among radioactive isotopes would reduce time and resources lost to false alarms.

On September 11, 2006, DNDO and CBP released the Radiation Portal Monitor Project Execution Plan (PEP). The PEP defines the overall project objectives, work scope, schedules, costs, and required funding for deploying radiation portal monitors, including Advanced Spectroscopic Portals, and calls for the construction of 1,034 portals. However, DNDO is updating the Joint DNDO/CBP Deployment Strategy to deploy 717 Advanced Spectroscopic Portals by July 31, 2013. Once the new strategy is approved, a new version of the PEP will be published that coincides with the joint deployment strategy.

As of May 31, 2008, the Advanced Spectroscopic Portal program had 41 government and contract staff assigned, and the current program manager said that the program is appropriately staffed. The Advanced Spectroscopic Portal program has evolved through numerous performance specification versions as the developing technology has matured. The current version is in a performance testing phase, with planned completion in fall 2008.

Before deploying the Advanced Spectroscopic Portal system, the DHS Secretary must certify that the system is a significant improvement in operational effectiveness over existing equipment. DNDO expects the Secretary to certify the system by fall 2008, with operational deployment

## **Appendix C**

### **Status of Programs and Systems from the DHS Plan**

---

following shortly thereafter. CBP plans to complete the operational deployment of the Radiation Portal Monitor system with both PVT and Advanced Spectroscopic Portal systems by the end of 2014.

From 2006 through 2007, GAO issued three reports related to the Advanced Spectroscopic Portal. These audits made eight recommendations, of which five were open as of May 31, 2008. DNDO disagreed with two of the five open recommendations. The open issues relate primarily to conducting cost-benefit analyses and realistic testing of the portals. In September 2008, GAO issued a report which made three recommendations relating to cost issues. Currently, GAO has an audit of Advanced Spectroscopic Portal in progress relating to nuclear detection architecture, testing, and cost. GAO provided the preliminary results of this audit in Congressional testimony in September 2008.

#### **Cargo Advanced Automated Radiography System**

The Cargo Advanced Automated Radiography System is a next-generation nonintrusive inspection system that would detect both conventional contraband and high-Z materials within cargo. High-Z materials are elements with high atomic numbers, including both special nuclear materials and materials that can be used to shield them. Thus, the system would be able to distinguish between low-density nonthreat materials, such as aluminum and foodstuffs, and high-density materials. These characteristics would improve CBP's ability to identify concealed and shielded special nuclear materials. Furthermore, this technology would automate the image processing required to detect high-density objects. This ability can be combined with the current ability to detect low-density contraband with little impact on CBP operators. With these advances, CBP and DNDO hope that the Cargo Advanced Automated Radiography System will enhance security while minimizing impact on legitimate commerce.

In September 2006, DNDO awarded three concept-of-design contracts for a 2-year development period. In 2008, major changes to the Cargo Advanced Automated Radiography System strategy were implemented in response to evolving DHS requirements, concurrent efforts in the commercial market, and difficulties in developing the technology. CBP and DNDO established the Joint Integrated Non-Intrusive Inspection program and working group to coordinate future development and testing of systems, including the Cargo Advanced Automated Radiography System. By June 2008, the working group had met four times, and the DNDO had five staff assigned to the project.



## **Appendix C**

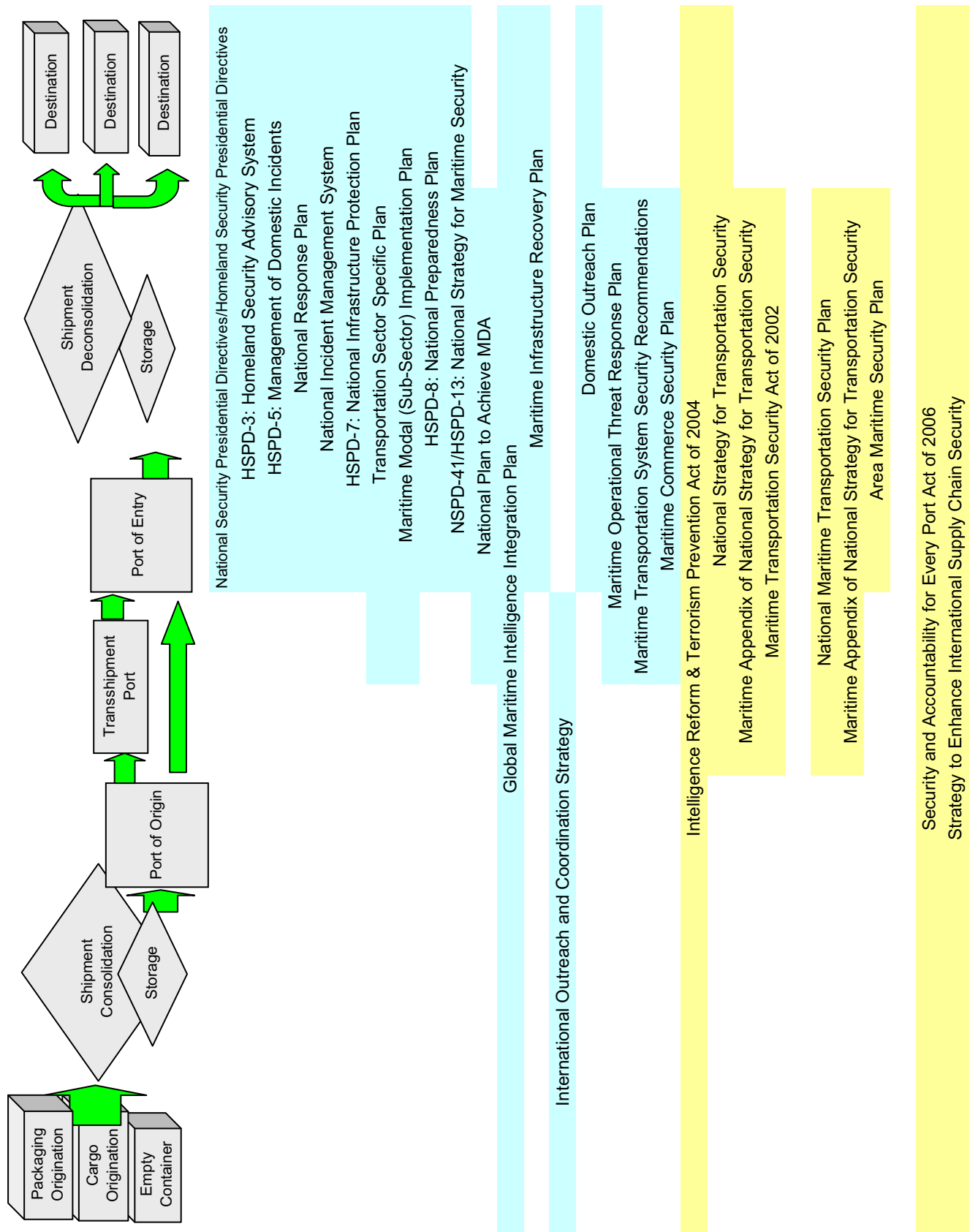
### **Status of Programs and Systems from the DHS Plan**

---

As of June 2008, the acquisition requirements were removed from the three system contracts. However, program management is still negotiating the contract modification for the remaining research and development. The three contracts for the system have either been completed or are approaching the critical design review phase.

The strategic benefits of the system course correction will be to establish a baseline detection capability for all hardware and software before entering any large-scale acquisition programs in the future. The FY 2008 planned accomplishments include initiating a test campaign to fully characterize the ability of commercially available nonintrusive inspection systems to manually detect shielded nuclear material. The FY 2009 goals include completion of developmental tests and evaluations of the system prototypes and a cost-benefit analysis of the entire program.

DNDO and CBP seek to design, develop, and test the system and to deploy the technology at CBP ports of entry as part of a multilayered system of radiation detection. Eventually, the system will be used to scan containers for high-Z materials at all CBP ports of entry, but as of May 31, 2008, the program remains in development and testing.



**Appendix E**  
**Major Contributors to This Report**

---

Paul Wood, Director for Trade Operations  
Gene Wendt, Audit Manager  
Elizabeth Garcia, Auditor in Charge  
Victoria Phan, Program Analyst  
Victor Leung, Program Analyst  
Andrew Smith, Program Analyst  
Corneliu Buzesan, Program Analyst

**Appendix F**  
**Report Distribution**

---

**Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chief of Staff  
General Counsel  
Executive Secretary  
Director, GAO/OIG Liaison Office  
Assistant Secretary for Office of Policy  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Office of Legislative Affairs  
Commissioner, Customs and Border Protection  
OIG Liaison, Customs and Border Protection  
Commandant, Coast Guard  
OIG Liaison, Coast Guard  
Director, Domestic Nuclear Detection Office  
OIG Liaison, Domestic Nuclear Detection Office

**Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees, as appropriate



#### ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at [www.dhs.gov/oig](http://www.dhs.gov/oig).

#### OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at [DHSOIGHOTLINE@dhs.gov](mailto:DHSOIGHOTLINE@dhs.gov); or
- Write to us at:  
DHS Office of Inspector General/MAIL STOP 2600,  
Attention: Office of Investigations - Hotline,  
245 Murray Drive, SW, Building 410,  
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.