United States Government Accountability Office

GAO

Statement before the Committee on Commerce, Science and Transportation, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, December 2, 2009

HOMELAND SECURITY

DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity

Statement for the Record
Cathleen A. Berrick, Managing Director
Homeland Security and Justice

December 2, 2009

HOMELAND SECURITY

DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-10-106, Statement Before the Committee on Commerce, Science and Transportation, U.S. Senate

Why GAO Did This Study

Securing the nation's transportation and information systems is a primary responsibility of the Department of Homeland Security (DHS). Within DHS, the Transportation Security Administration (TSA) is responsible for securing all transportation modes; U.S. Customs and Border Protection (CBP) is responsible for cargo container security; the U.S. Coast Guard is responsible for protecting the maritime environment; and the National Protection and Programs Directorate is responsible for the cybersecurity of critical infrastructure. This statement focuses on the progress and challenges DHS faces in key areas of maritime, aviation, and cybersecurity. It is based on GAO products issued from June 2004 through November 2009, as well as ongoing work on air cargo security. GAO reviewed relevant documents; interviewed cognizant agency officials; and observed operations at 12 airports, chosen by size and other factors. The results are not generalizable to all airports.

What GAO Recommends

GAO is not making recommendations in this statement; however, GAO has made prior recommendations to DHS to, among other things, analyze the feasibility of scanning U.S.-bound cargo containers and more fully protect computer-reliant critical infrastructures. DHS generally agreed with these recommendations. DHS provided technical comments on this statement, which GAO incorporated as appropriate.

View GAO-10-106T or key components.

For more information, contact Cathleen Berrick at (202) 512-8777 or berrickc@gao.gov.

What GAO Found

DHS has made progress in enhancing security in the maritime sector, but key challenges remain. For example, as part of a statutory requirement to scan 100 percent of U.S.-bound container cargo by July 2012, CBP has implemented the Secure Freight Initiative at select foreign ports. However, CBP does not have a plan for fully implementing the 100 percent scanning requirement by July 2012 because it questions the feasibility, although it has not performed a feasibility analysis of the requirement. Rather, CBP has planned two new initiatives to further strengthen the security of container cargo, but these initiatives will not achieve 100 percent scanning. Further, TSA, the Coast Guard, and the maritime industry took a number of steps to enroll over 93 percent of the estimated 1.2 million users in the Transportation Worker Identification Credential (TWIC) program (designed to help control access to maritime vessels and facilities) by the April 15, 2009 compliance deadline, but they experienced challenges resulting in delays and in ensuring the successful execution of the TWIC pilot. While DHS and the Coast Guard have developed a strategy and programs to reduce the risks posed by small vessels, they face ongoing resource and technology challenges in tracking small vessels and preventing attacks by such vessels.

In the aviation sector, TSA has made progress in meeting the statutory mandate to screen 100 percent of air cargo transported on passenger aircraft by August 2010 and in taking steps to strengthen airport security, but TSA continues to face challenges. TSA's efforts include developing a system to allow screening responsibilities to be shared across the domestic air cargo supply chain, among other steps. Despite these efforts, TSA and the industry face a number of challenges including the voluntary nature of the program, and ensuring that approved technologies are effective with air cargo. TSA also does not expect to meet the mandated 100 percent screening deadline as it applies to air cargo transported into the U.S., in part due to existing screening exemptions for this type of cargo and challenges in harmonizing security standards with other nations. GAO is reviewing these issues as part of its ongoing work and will issue a final report next year. In addition, TSA has taken a variety of actions to strengthen airport security by, among other things, implementing a worker screening program; however, TSA still faces challenges in this area.

DHS has made progress in strengthening cybersecurity, such as addressing some lessons learned from a cyber attack exercise, but further actions are warranted. Since 2005, GAO has reported that DHS has not fully satisfied its key responsibilities for protecting the nation's computer-reliant critical infrastructures and has made related recommendations to DHS, such as bolstering cyber analysis and warning capabilities and strengthening its capabilities to recover from Internet disruptions. DHS has since developed and implemented certain capabilities to satisfy aspects of its responsibilities, but it has not fully implemented GAO's recommendations and, thus, more action is needed to address the risk to critical cybersecurity infrastructure.

Mr. Chairman and Members of the Committee:

I am pleased to submit this statement on the progress that the Department of Homeland Security (DHS) has made and the challenges it faces in key areas of maritime and aviation security, as well as in securing the nation against computer-based, or cyber attacks. The economic well being of the United States is dependent on the expeditious flow of people and goods through the U.S. transportation system, which moves millions of passengers and tons of freight each day. The extensiveness of the transportation system, as well as the sheer volume of passengers and freight moved, makes it both an attractive target and challenging to secure. Ports, waterways, and vessels are part of an economic engine handling more than $700 billion in merchandise annually, and an attack on this system could have a widespread impact on global shipping, international trade, and the global economy. Likewise, successful terrorist attacks and plots against the commercial aviation system in the past 8 years highlight the threats and vulnerabilities this system faces. Balancing security concerns with the need to facilitate the free flow of people and commerce remains an ongoing challenge for the public and private sectors alike. Likewise, pervasive and sustained cyber attacks against the United States and others continue to pose a potentially devastating impact to systems and operations and the critical infrastructures that they support.

Within DHS, numerous component agencies have responsibility for securing areas of transportation security and computer-reliant critical infrastructures, such as communications and electricity. The Transportation Security Administration (TSA) is the federal agency with primary responsibility for securing all modes of transportation and has developed and implemented a variety of programs and procedures to secure commercial aviation and surface modes of transportation. U.S. Customs and Border Protection (CBP) has a priority mission of keeping terrorists and their weapons out of the U.S., is responsible for securing and facilitating trade, and has primary responsibility for cargo container security. The Coast Guard has responsibility for protecting the public, the environment, and U.S. economic and security interests in any maritime region in which those interests may be at risk, including America's coasts, ports, and inland waterways. The National Protection and Programs Directorate is responsible for, among other things, assuring the security, resiliency, and reliability of the nation's computer-reliant critical infrastructures—a practice known as cyber critical infrastructure protection, or cyber CIP.

A number of laws have been enacted in recent years to strengthen maritime and aviation security, as well as cybersecurity. In response to provisions of the Aviation and Transportation Security Act (ATSA), TSA established the Transportation Worker Identification Credential (TWIC) program in December 2001.[1] The Security and Accountability For Every (SAFE) Port Act of 2006 directed the Secretary of Homeland Security to, among other things, implement the TWIC pilot project in the maritime sector.[2] To increase the security of container cargo bound for the United States, the SAFE Port Act further required CBP to establish a pilot program to test the feasibility of scanning 100 percent of U.S.-bound containers at foreign ports.[3] Further, in August 2007 the Implementing Recommendations of the 9/11 Commission Act (9/11 Act) was enacted and provides, among other things, that by July 2012, a container loaded on a vessel in a foreign port shall not enter the United States unless that container is scanned before it is loaded onto the vessel.[4] The Act further requires that by August 2010, 100 percent of cargo—domestic and inbound—transported on passenger aircraft be physically screened.[5] To address the threats posed by cyber attacks, President Bush issued a 2003 national strategy and related policy directives aimed at improving cybersecurity nationwide, including both government systems and those

[1]See Pub. L. No. 107-71, 115 Stat. 597 (2001). TSA was transferred from the Department of Transportation to DHS pursuant to requirements in the Homeland Security Act of 2002. See Pub. L. No. 107-296, § 403(2), 116 Stat. 2135, 2178.

[2]See Pub. L. No. 109-347, 120 Stat. 1884.

[3]See id. § 231, 120 Stat. at 1915 (codified at 6 U.S.C. § 981).

[4]See Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (2007) (amending 6 U.S.C. § 982(b)). Both the SAFE Port Act and 9/11 Act define scanning to be an examination with both non-intrusive imaging equipment and radiation detection equipment. In addition, while the law states that cargo containers are not to enter the United States unless they were scanned at a foreign port, actual participation in the program by sovereign foreign governments and ports is voluntary.

[5]The 9/11 Act establishes minimum standards for screening air cargo and defines screening for purposes of the air cargo screening mandate as a physical examination or nonintrusive methods of assessing whether cargo poses a threat to transportation security. See Pub. L. No. 110-53, § 1602(a), 121 Stat. at 477-79 (codified at 49 U.S.C. § 44901(g)). Solely performing a review of information about the contents of cargo or verifying the identity of the cargo's shipper does not constitute screening for purposes of satisfying the mandate. For the purposes of this statement, domestic air cargo refers to cargo transported by air within the United States and from the United States to a foreign location by both U.S. and foreign-based air carriers; and inbound cargo refers to cargo transported by U.S. and foreign-based air carriers from a foreign location to the United States.

that support cyber critical infrastructures[6] owned and operated by the private sector.[7]

My testimony today focuses on the progress that DHS and its component agencies have made to strengthen maritime, aviation, and cybersecurity, and the challenges that remain. In particular, I will address (1) cargo container scanning, (2) efforts to enroll maritime workers in the TWIC program, (3) small vessel security,[8] (4) air cargo screening, (5) airport perimeter and access control security, and (6) cybersecurity for critical infrastructure.

My comments are based on related GAO reports and testimonies issued from June 2004 through November 2009,[9] as well as ongoing work that will be completed in early 2010 assessing the progress that DHS and its component agencies have made in addressing challenges related to air cargo screening. To conduct this work, we reviewed relevant documents related to the programs reviewed; interviewed cognizant DHS, TSA, Coast Guard, and CBP officials; and observed operations at a non-probability sample of 19 seaports—13 domestic and 6 foreign—and 12 airports, chosen by size, program participation, and other factors. Although the results of our site visits are not generalizable to all seaports, airports, or officials, we gained a critical understanding of the progress and challenges associated with implementing efforts to secure the transportation system and improve cyber CIP. We have conducted our ongoing work—covering the period October 2008 to date—as well as the prior audit work that serves as the basis for this statement, in accordance with generally

[6]Critical infrastructures are systems and assets, whether physical or virtual, so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters.

[7]The White House, The National Strategy to Secure Cyberspace (Washington, D.C.: February 2003); Homeland Security Presidential Directive 7 (Washington, D.C.: Dec. 17, 2003); and National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

[8]According to DHS's *Small Vessel Security Strategy*, "small vessels" are characterized as any watercraft—regardless of method of propulsion—less than 300 gross tons, and used for recreational or commercial purposes.

[9]See for example, GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, GAO-09-399 (Washington, D.C.: Sept. 30, 2009) and *Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed*, GAO-09-337 (Washington, D.C.: Mar. 17, 2009).

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives.

In summary, DHS has made progress in enhancing security in the maritime sector, but key challenges remain. Among other things, CBP has begun working with foreign ports to scan U.S.-bound container cargo; TSA, Coast Guard, and the maritime industry enrolled over 93 percent of the estimated 1.2 million users in the TWIC program by the April 15, 2009 compliance deadline; and DHS and the Coast Guard have developed a strategy and programs to reduce the risks associated with small vessels. However, DHS and its component agencies face a number of management, technological, and resource challenges associated with these efforts. In our previous work, we made recommendations to help address these challenges. Specifically, in our October 2009 report on scanning of U.S.-bound cargo containers, we made recommendations to DHS and CBP to complete a feasibility analysis, cost estimates, and a cost-benefit analysis and provide the results to Congress to help strengthen container security. In our November 2009 report on TWIC, we made recommendations to TSA to, among other things, expedite the development of contingency and disaster recovery plans and system(s), and recommended to TSA and the Coast Guard that they develop a detailed evaluation plan to help ensure that needed information on biometrics readers will result from the pilot. DHS generally concurred and discussed actions to implement recommendations from both of these reports, but we believe that these actions will not fully address the intent of all of the recommendations. In the aviation sector, TSA has made progress in meeting the air cargo screening mandate of the 9/11 Act—including developing a program to share screening responsibilities across the supply chain, but the agency continues to face challenges related to planning and technology, among other things. In our September 2009 report on airport security, we made recommendations to TSA to, among other things, develop a national strategy to guide stakeholder efforts to strengthen airport perimeter and access control security, to which DHS concurred. Finally, regarding cyber CIP issues, DHS has developed and implemented certain capabilities to satisfy aspects of its cybersecurity responsibilities, such as addressing certain lessons learned from cyber attack exercises, but it has not fully satisfied our recommendations to, among other things, bolster cyber analysis and warning capabilities and strengthen its capabilities to recover from Internet disruptions. As a result, DHS needs to take further action to address these areas.

Background

Secure Freight Initiative (SFI)

In December 2006, in response to SAFE Port Act requirements, DHS, and the Department of Energy (DOE) jointly announced the formation of the Secure Freight Initiative (SFI) pilot program to test the feasibility of scanning 100 percent of U.S.-bound container cargo at three foreign ports (Puerto Cortes, Honduras; Qasim, Pakistan; and Southampton, United Kingdom). According to CBP officials, while initiating the SFI program at these ports satisfied the SAFE Port Act requirement, CBP also selected the ports of Busan, South Korea; Hong Kong; Salalah, Oman; and Singapore to more fully demonstrate the capability of the integrated scanning system at larger, more complex ports. As of October 2009, SFI has been operational at five of these initial seven seaports. According to CBP and DOE officials, the SFI program builds upon existing container security measures by enhancing the U.S. government's ability to have containers scanned for nuclear and radiological material overseas and, thus, better assess the risk of weapons of mass destruction (WMD) in inbound cargo containers.

Transportation Worker Identification Credential (TWIC)

Managed by TSA and the U.S. Coast Guard, the TWIC program aims to protect the nation's maritime transportation facilities and vessels by requiring maritime workers to complete background checks and obtain a biometric identification card in order to gain unescorted access to the secure areas of regulated facilities and vessels.[10] A federal regulation in January 2007 set a compliance deadline, subsequently extended to April 15, 2009, whereby each maritime worker was required to hold a TWIC in order to obtain unescorted access to secure areas of regulated facilities

[10]Biometrics refers to technologies that measure and analyze human body characteristics—such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements—for authentication purposes. According to Coast Guard guidance, a secure area is an area that has security measures in place for access control. For most maritime facilities, the secure area is generally any place inside the outer-most access control point. For a vessel or outer continental shelf facility, such as off-shore petroleum or gas production facilities, the secure area is generally the whole vessel or facility.

and vessels.[11] In addition, TSA has initiated a pilot to test the use of TWIC with related access control technologies.

Small Vessel Security

Concerns have grown about the security risks of small vessels and DHS has identified the four gravest risk scenarios involving the use of such vessels for terrorist attacks. Some of these risks have been shown to be real through attacks conducted outside U.S. waters, but to date, no small boat attacks have happened in the United States. These four scenarios include the use of a small vessel as (1) a waterborne improvised explosive device, (2) a means of smuggling weapons into the United States, (3) a means of smuggling humans into the United States, and (4) a platform for conducting a stand-off attack.

Air Cargo Security

Air cargo ranges in size from 1 pound to several tons, and can be shipped in various forms, including unit load devices (ULD) that allow many packages to be consolidated into one container or pallet, wooden crates, or individually wrapped/boxed pieces, known as loose or bulk cargo. Participants in the air cargo shipping process include shippers, such as manufacturers; freight forwarders, who consolidate cargo from shippers and take it to air carriers for transport; air cargo handling agents, who process and load cargo onto aircraft on behalf of air carriers; and air carriers that load and transport cargo.[12] TSA's responsibilities include, among other things, establishing security requirements governing domestic and foreign passenger air carriers that transport cargo, and domestic freight forwarders.

Perimeter and Access Control Security

Airport perimeter and access control security is intended to prevent unauthorized access into secured airport areas, either from outside the airport complex or from within. Airport operators generally have direct

[11]To implement the requirement for using a biometric credential for accessing select maritime facilities and vessels—as called for in the Maritime Transportation Security Act of 2002 (MTSA), as amended by the Security and Accountability For Every (SAFE) Port Act of 2006—the credential rule (72 Fed. Reg. 3492 (2007)) established that all maritime workers requiring unescorted access to secure areas of MTSA-regulated facilities and vessels were expected to hold TWICs by September 25, 2008, but the final compliance date was extended to April 15, 2009, pursuant to 73 Fed. Reg. 25562 (2008).

[12]For purposes of this statement, the term freight forwarders only includes those freight forwarders that are regulated by TSA, also referred to as indirect air carriers.

day-to-day responsibility for maintaining and improving perimeter and access control security, as well as implementing measures to reduce worker risk. However, TSA has primary responsibility for establishing and implementing measures to improve security operations at U.S. commercial airports—that is, TSA-regulated airports—including overseeing airport operator efforts to maintain perimeter and access control security.[13] Airport workers may access sterile areas— areas of airports where passengers wait after screening to board departing aircraft— through TSA security checkpoints or through other access points that are secured by the airport operator. The airport operator is also responsible, in accordance with its security program, for securing access to secured airport areas where passengers are not permitted. Airport methods used to control access vary, but all access controls must meet minimum performance standards in accordance with TSA requirements.

Cybersecurity

The federal government has developed a strategy to address cyber threats. Specifically, President Bush issued the 2003 National Strategy to Secure Cyberspace and related policy directives, such as Homeland Security Presidential Directive 7, that specify key elements of how the nation is to secure key computer-based systems, including both government systems and those that support critical infrastructures owned and operated by the private sector. The strategy and related policies also establish DHS as the focal point for cyber critical infrastructure protection and assigns DHS multiple leadership roles and responsibilities in this area, to include (1) developing a comprehensive national plan for critical infrastructure protection, including cybersecurity; (2) developing and enhancing national cyber analysis and warning capabilities; (3) providing and coordinating incident response and recovery planning, including conducting incident response exercises; (4) identifying, assessing, and supporting efforts to reduce cyber threats and vulnerabilities, including those associated with infrastructure control systems; and (5) strengthening international cyberspace security. More recently, in February 2009, President Obama directed the National Security Council and Homeland Security Council to conduct a comprehensive review to assess the United States' cybersecurity-related policies and structures. The resulting May 2009

[13]See generally Pub. L. No. 107-71, 115 Stat. 597 (2001).

report made a number of recommendations to improve the nation's approach.[14]

Maritime Security

CBP Has Made Some Progress in Working with Foreign Ports to Scan U.S.-Bound Containers, but Challenges Remain in Expanding the Program to Larger Ports and Meeting the Statutory Target Date

In October 2009, we reported that CBP has made some progress in working with the initial SFI ports to scan U.S.-bound cargo containers; but because of challenges to expanding scanning operations, especially to larger ports, the feasibility of scanning 100 percent of U.S.-bound cargo containers at over 600 foreign seaports remains largely unproven.[15] CBP and DOE have been successful in integrating images of scanned containers onto a single computer screen that can be reviewed remotely from the United States and have also been able to use these initial ports as a test bed for new applications of existing technology, such as mobile radiation scanners. However, the SFI ports' level of participation, in some cases, has been limited in terms of duration or scope. While 54 to 86 percent of the U.S.-bound cargo containers, on average, were scanned at 3 comparatively low volume ports that are responsible for less than 3 percent of container shipments to the United States, CBP has not been able to achieve sustained scanning rates above 5 percent at 2 comparatively larger ports—the type of ports that ship most containers to the United States.[16] Scanning operations at the initial SFI ports have encountered a number of challenges, such as logistical problems with containers transferred from rail or other vessels, and CBP officials are concerned that they and the participating ports cannot overcome them.

CBP has developed two initiatives related to SFI for improving container security; however, challenges remain as neither initiative will enable CBP to fully achieve the 9/11 Act requirement to scan 100 percent of all U.S.-

[14]The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

[15]GAO, *Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers*, GAO-10-12 (Washington, D.C.: Oct. 30, 2009).

[16]Scanning percentages at Port Qasim, Puerto Cortes, and the Port of Southampton reflect operations conducted from November 2007 through May 2009.Scanning percentages at the Port of Hong Kong reflect operations conducted from February 2008 through April 2009. Scanning percentages at the Port of Busan reflect operations conducted from April 2009 through May 2009.

bound cargo by July 2012. The first initiative, the "strategic trade corridor strategy," involves scanning 100 percent of U.S.-bound containers at selected foreign ports where CBP believes it will mitigate the greatest risk of weapons of mass destruction (WMD) entering the United States. The Secretary of Homeland Security approved this strategy and, according to CBP, is in negotiations with foreign governments to expand SFI to ports in those countries. The second initiative, known as "10+2", requires importers to provide 10 data elements and vessel carriers to provide 2 data elements on containers and their cargo to CBP, which provides further information to CBP, thus, improving its ability to identify containers that may pose a risk of containing WMD for additional scrutiny—such as scanning or physical inspection. Based on discussions with DHS and CBP officials, it is unclear whether DHS intends for the strategic trade corridor strategy and 10+2 to be implemented in lieu of the 100 percent scanning requirement or whether it is the first phase of implementation. While these initiatives may collectively improve container security, they will not enable CBP to fully achieve the 9/11 Act requirement to scan 100 percent of U.S.-bound containers by July 2012. According to CBP, it does not have a plan for fully implementing the scanning requirement by this date because it questions the feasibility; however, it has not performed a feasibility analysis of expanding 100 percent scanning, as required by the SAFE Port Act. To address this, in October 2009, we recommended that CBP conduct a feasibility analysis of implementing 100 percent scanning and provide the results, as well as alternatives to Congress, in order to determine the best path forward to strengthen container security.[17] CBP concurred with our recommendation. Further, senior DHS and CBP officials acknowledge that most, if not all foreign ports, will not be able to meet the July 2012 target date for scanning all U.S.-bound cargo. As a result, DHS has recently decided to grant a blanket extension to all foreign ports, thus extending the target date for compliance with this requirement by 2 years, to July 2014.

[17]GAO-10-12.

TSA and the Coast Guard Took Steps to Enroll Transportation Workers into the TWIC Program by the Mandated Deadline, but Challenges in Program Scheduling and Evaluation May Hinder the TWIC Reader Pilot's Usefulness

In November 2009 we reported that, based on lessons learned from its early experiences with enrollment and activation, TSA and its contractor took steps to prepare for a surge in TWIC enrollments and activations as local compliance dates approached.[18] For example, according to TSA and port facility representatives, TSA and its contractor increased enrollment center resources, such as increasing the number of enrollment and activation stations to meet projected TWIC user demands. Likewise, the Coast Guard employed strategies to help the maritime industry meet the TWIC national compliance date while not disrupting the flow of commerce. As a result of these efforts, TSA reported enrolling 1,121,461 workers in the TWIC program, or over 93 percent of the estimated 1.2 million users, by the April 15, 2009 deadline.

Although most workers received their TWICs, TSA data show that some workers experienced delays in receiving TWICs. Among the reasons for the delays was that a power failure occurred in October 2008 at the government facility that processes TWIC data that caused a hardware component failure in the TWIC enrollment and activation system for which no replacement component was on hand. In our November 2009 report on TWIC, we made recommendations to TSA to expedite the development of contingency and disaster recovery plans and system(s). DHS stated it is taking steps to address this recommendation and future potential TWIC system failures by developing a system to support disaster recovery by 2012. While DHS's efforts are a positive step, until they are complete, TWIC systems remain vulnerable to similar disasters.

In response to our 2006 recommendation and a SAFE Port Act requirement, TSA initiated a pilot in August 2008[19] known as the TWIC reader pilot, to test TWIC-related access control technologies.[20] The pilot is expected to test the viability of selected biometric card readers for use in reading TWICs within the maritime environment and test the technical aspects of connecting TWIC readers to access control systems. The results

[18]GAO, *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers*, GAO-10-43 (Washington, D.C.: Nov. 18, 2009).

[19]The pilot initiation date is based on the first date of testing identified in the TWIC pilot schedule. The SAFE Port Act required the pilot to commence no later than 180 days after the date of enactment of the SAFE Port Act (October 13, 2006).

[20]GAO, *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, GAO-06-982 (Washington, D.C.: Sept. 29, 2006).

of the pilot are expected to inform the development of the card reader rule requiring TWIC readers for use in controlling access at MTSA regulated vessels/facilities. Based on the August 2008 pilot initiation date, the card reader rule is to be issued no later than 24 months from the initiation of the pilot, or by August 2010.

Although TSA has made significant progress to incorporate best practices into TWIC's schedule for implementing the reader pilot program, weaknesses continue to exist that limit TSA's ability to use the schedule as a management tool to guide the pilot and accurately identify the pilot's completion date. In response to limitations that we identified, the program office developed a new TWIC pilot master schedule in March 2009, and updated it in April 2009, and again in May 2009. The pilot schedule went from not meeting any of the nine scheduling best practices in September 2008 to fully addressing one of the practices, addressing seven practices to varying degrees, and not addressing one practice.[21] While TSA has improved its technical application of program scheduling practices on the TWIC reader pilot program, as of May 2009, weaknesses remain that may adversely impact its usefulness as a management tool. For example, the schedule does not accurately reflect all key pilot activities or assign resources to those activities. To address these weaknesses, in our November 2009 report we recommended that TSA, in concert with pilot participants, fully incorporate best practices for program scheduling in the pilot. TSA concurred in part with our recommendation. In addition, shortfalls in TWIC pilot planning have presented a challenge for TSA and the Coast Guard in ensuring that the pilot is broadly representative of deployment conditions. This is in part because an evaluation plan that

[21]These best practices include (1) capturing all activities—defining in detail the work to be completed, including activities to be performed; (2) sequencing all activities—listing activities in the order in which they are to be carried out; (3) assigning resources to all activities—identifying the resources needed to complete the activities; (4) establishing the duration of all activities—determining how long each activity will take to execute; (5) integrating all activities horizontally and vertically—achieving aggregated products or outcomes by ensuring that products and outcomes associated with other sequenced activities are arranged in the right order, and dates for supporting tasks and subtasks are aligned; (6) establishing the critical path for all activities—identifying the path in the schedule with the longest duration through the sequenced list of key activities; (7) identifying float between activities—using information on the amount of time that a predecessor activity can slip before the delay affects successor activities; (8) conducting a schedule risk analysis—using statistical techniques to predict the level of confidence in meeting a project's completion date; and (9) updating the schedule using logic and durations to determine the dates for all activities—continuously updating the schedule to determine realistic start and completion dates for program activities based on current information.

fully identifies the scope of the pilot and the methodology for collecting and analyzing the information resulting from the pilot has not been developed. Agency officials told us that no such evaluation plan was developed because they believe that the existing pilot documentation coupled with subject matter expertise would be sufficient to guide the pilot. However, our review of the TWIC pilot highlights weaknesses that could be rectified by the development and use of an evaluation plan. To address this, in November 2009, we recommended that TSA and the Coast Guard develop an evaluation plan to help ensure that needed information on the use of biometrics readers will result from the pilot. DHS concurred and discussed actions to implement the recommendation, but it is too early to determine if the intended actions will fully address the intent of the recommendation.

DHS and Coast Guard Have a Strategy and Programs in Place, but Identifying and Preventing Small Vessel Attacks Remains a Challenge

While DHS and the Coast Guard have developed a strategy and programs to reduce the risks associated with small vessels, they face ongoing challenges in tracking small vessels and preventing attacks by such vessels.[22] In April 2008, DHS issued its Small Vessel Security Strategy and is now in the process of developing and reviewing a more detailed implementation plan. After review by the Coast Guard and CBP, the draft plan was forwarded to DHS on September 18, 2009 with a recommendation for approval, but DHS has not yet issued a final decision. As part of its effort to improve security in the maritime domain, the Coast Guard is also implementing two major unclassified systems to track a broad spectrum of vessels. While these systems use proven technologies, they depend on the compliance of vessel operators to carry equipment needed to interact with these systems and to make sure the systems are turned on and functioning properly. These systems, however, generally cannot track small vessels. The Coast Guard and other agencies have other systems, though—which can include cameras and radars—that can track small vessels within ports, but these systems are not installed at all ports, and do not always work in bad weather or at night. In addition, the Coast Guard and other agencies, such as the New Jersey State Police, have several programs in place to address risks from small vessels, such as outreach efforts to the boating community to share threat information. However, the Coast Guard program faces resource limitations. For

[22]For further information on the risks associated with small vessels, see GAO, *Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed*, GAO-09-337 (Washington, D.C.: Mar. 17, 2009).

example, the Coast Guard's program to reach out to the boating community for their help in detecting suspicious activity, America's Waterway Watch, lost the funding it received through a Department of Defense readiness training program for military reservists in fiscal year 2008. Now it must depend on the activities of the Coast Guard Auxiliary, a voluntary organization, for most of its outreach efforts. Even with systems in place to track small vessels, there is widespread agreement among maritime stakeholders that it is very difficult to detect threatening activity by small vessels without prior knowledge of a planned attack.

Aviation Security

TSA Has Made Progress in Meeting the Air Cargo Screening Mandate, but Still Faces Participation, Technology, Oversight, and Inbound Cargo Challenges

As we previously reported in March 2009, TSA has taken several key steps to meet the air cargo screening mandate of the 9/11 Act as it applies to domestic cargo.[23] TSA's approach involves multiple air cargo industry stakeholders sharing screening responsibilities across the air cargo supply chain. According to TSA officials, this decentralized approach is expected to minimize carrier delays, cargo backlogs, and potential increases in cargo transit time, which would likely result if screening were conducted primarily by air carriers at the airport. The specific steps that TSA has taken to address domestic air cargo screening include the following:

- **Revised air carrier security programs:** Effective October 1, 2008, TSA established a requirement for 100 percent screening of nonexempt cargo transported on narrow-body passenger aircraft.[24] Effective February 1, 2009, TSA also required air carriers to ensure the screening of 50 percent of all nonexempt air cargo transported on all passenger aircraft. Furthermore, effective February 2009, TSA revised or eliminated most of its screening exemptions for domestic cargo.[25]

[23]GAO, *Aviation Security: Preliminary Observations on TSA's Progress and Challenges in Meeting the Statutory Mandate for Screening Air Cargo on Passenger Aircraft*, GAO-09-422T (Washington, D.C.: Mar.18, 2009).

[24]Narrow-body flights transport about 26 percent of all cargo on domestic passenger flights. According to TSA officials, narrow-body aircraft make up most domestic passenger flights, and transport most passengers traveling on domestic passenger flights.

[25]Effective September 2009, TSA revised or eliminated additional exemptions for domestic cargo.

- **Created the Certified Cargo Screening Program (CCSP):** TSA created a voluntary program to allow screening to take place earlier in the shipping process and at various points in the air cargo supply chain—including before the cargo is consolidated. In this program, air cargo industry stakeholders—such as freight forwarders and shippers—voluntarily apply to become certified cargo screening facilities (CCSF). CCSFs in the program were required to begin screening cargo as of February 1, 2009.

- **Issued an interim final rule:** On September 16, 2009, TSA issued an interim final rule, effective November 16, 2009, that among other things, codifies the statutory air cargo screening requirements of the 9/11 Act and establishes requirements for entities participating in the CCSP.

- **Established the Air Cargo Screening Technology Pilot:** To operationally test explosives trace detection (ETD) and X-ray technology among CCSFs, TSA created the Air Cargo Screening Technology Pilot in January 2008, and selected some of the largest freight forwarders to use the technologies and report on their experiences.[26] This pilot is ongoing, with an anticipated end date of August 2010, and the results have not yet been finalized.

- **Expanded its explosives detection canine program:** To assist air carriers in screening cargo, TSA has taken steps to expand the use of TSA-certified explosives detection canine teams. TSA now has 120 allocated canine teams dedicated to air cargo screening at 20 major airports.

While these steps are encouraging, TSA faces several challenges in meeting the air cargo screening mandate. First, although industry participation in the CCSP is vital to TSA's approach to move screening responsibilities across the supply chain, the voluntary nature of the program may make it difficult to attract program participants needed to screen the required levels of domestic cargo. Attracting certified cargo screening facilities (CCSF) is important because much cargo is currently delivered to air carriers in a consolidated form and the requirement to screen individual pieces of cargo will necessitate screening earlier in the air cargo supply chain. However, there are concerns about potential

[26]ETD requires human operators to collect samples of items to be screened with swabs, which are chemically analyzed to identify any traces of explosives material.

program costs, including acquiring expensive technology, hiring additional personnel, conducting additional training, and making facility improvements.

Second, while TSA has taken steps to test technologies for screening and securing air cargo, it has not yet completed assessments of the technologies it plans to allow air carriers and program participants to use in meeting the August 2010 screening mandate. According to TSA officials, the agency has conducted laboratory assessments and plans to complete operational testing of X-ray technologies by late 2009, and laboratory and operational testing of explosives trace detection technology by August 2010. However, these technologies, which have not yet been fully tested for effectiveness, are currently being used by industry participants to meet air cargo screening requirements.

Third, TSA faces challenges overseeing compliance with the CCSP due to the size of its current Transportation Security Inspector (TSI) workforce. Under the CCSP, in addition to performing inspections of air carrier and freight forwarders, TSIs are to also perform compliance inspections of new regulated entities that voluntarily become CCSFs, as well as conduct additional CCSF inspections of existing freight forwarders. TSA officials have stated that there may not be enough TSIs to conduct compliance inspections of all the potential CCSFs once the program is fully implemented by August 2010. Until TSA completes its staffing study, TSA may not be able to determine whether it has the necessary staffing resources to ensure that entities involved in the CCSP are meeting TSA requirements to screen and secure air cargo.[27]

Finally, TSA has taken some steps to meet the screening mandate as it applies to inbound cargo but does not expect to achieve 100 percent screening of inbound cargo by the August 2010 deadline. TSA revised its requirements to, in general, require carriers to screen 50 percent of nonexempt inbound cargo. TSA also began harmonization of security standards with other nations through bilateral and quadrilateral discussions.[28] In addition, TSA continues to work with CBP to leverage an

[27]For additional information on TSA's staffing study, see GAO, *Aviation Security: Status of Transportation Security Inspector Workforce*, GAO-09-123R (Washington D.C.: Feb. 6, 2009).

[28]The term harmonization is used to describe countries' efforts to coordinate their security practices to enhance security and increase efficiency by avoiding duplication of effort.

existing CBP system to identify and target high-risk air cargo. However, TSA does not expect to meet the mandated 100 percent screening level by August 2010. This is due, in part, to existing inbound screening exemptions, which TSA has not reviewed or revised, and to challenges TSA faces in harmonizing the agency's air cargo security standards with those of other nations. Moreover, TSA's international inspection resources are limited. We will continue to explore these issues as part of our ongoing review of TSA's air cargo security efforts, to be issued next year.

TSA Has Taken Actions to Strengthen Airport Security, but Faces Challenges in Assessing Risk, Evaluating Worker Screening Methods, Addressing Airport Technology Needs, and Developing a National Strategy for Airport Security

In our September 2009 report on airport security, we reported that TSA has implemented a variety of programs and protective actions to strengthen the security of commercial airports.[29] For example, in March 2007, TSA implemented a random worker screening program—the Aviation Direct Access Screening Program (ADASP)—nationwide to enforce access procedures, such as ensuring that workers do not possess unauthorized items when entering secured areas. In addition, TSA has expanded requirements for background checks and the population of individuals who are subject to these checks, and has established a statutorily directed pilot program to assess airport security technology.[30] In 2004 TSA initiated the Airport Access Control Pilot Program to test, assess, and provide information on new and emerging technologies, including biometrics. TSA issued a final report on the pilots in December 2006.

As we reported in September 2009, while TSA has taken numerous steps to enhance airport security, it continues to face challenges in several areas, such as assessing risk, evaluating worker screening methods, addressing airport technology needs, and developing a unified national strategy for airport security.[31] For example, while TSA has taken steps to assess risk related to airport security, it has not conducted a comprehensive risk assessment based on assessments of threats, vulnerabilities, and consequences, as required by DHS's National Infrastructure Protection Plan . To address these issues, we recommended, among other things, that TSA develop a comprehensive risk assessment of airport security and

[29]GAO-09-399.

[30]According to TSA officials, the agency established this program in response to a provision enacted through the Aviation and Transportation Security Act. See Pub. L. No.107-71 § 106(d), 115 Stat. at 610 (codified at 49 U.S.C. § 44903(c)(3)).

[31]GAO-09-399.

milestones for its completion, and evaluate whether the current approach to conducting vulnerability assessments appropriately assesses vulnerabilities. DHS concurred with these recommendations.

Further, to respond to the threat posed by airport workers, the Explanatory Statement accompanying the DHS Appropriations Act, 2008, directed TSA to use $15 million of its appropriation to conduct a pilot program at seven airports to help identify the potential costs and benefits of 100 percent worker screening and other worker screening methods.[32] In July 2009 TSA issued a final report on the results and concluded that random screening is a more cost-effective approach because it appears "roughly" as effective in identifying contraband items at less cost than 100 percent worker screening.[33] However, the report also identified limitations in the design and evaluation of the program and in the estimation of costs. Given the significance of these limitations, we reported in September 2009 that it is unclear whether random worker screening is more or less cost-effective than 100 percent worker screening.[34] In addition, TSA did not document key aspects of the pilot's design, methodology, and evaluation, such as a data analysis plan, limiting the usefulness of these efforts. To address this, we recommended that TSA ensure that future airport security pilot program evaluation efforts include a well-developed and well-documented evaluation plan, to which DHS concurred.

Moreover, although TSA has taken steps to develop biometric worker credentialing, it is unclear to what extent TSA plans to address statutory requirements regarding biometric technology, such as developing or requiring biometric access controls at airports, establishing comprehensive standards, and determining the best way to incorporate

[32]Explanatory Statement accompanying Division E of the Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, Div. E, 121 Stat. 1844, 2042 (2007), at 1048. While the Statement refers to these pilot programs as airport employee screening pilots, for the purposes of this statement, we use "worker screening" to refer to the screening of all individuals who work at the airport.

[33]Transportation Security Administration, *Airport Employee Screening Pilot Program Study: Fiscal Year 2008 Report to Congress* (Washington, D.C., July 7, 2009).

[34]The contractor TSA hired to assist with the pilot program identified design and evaluation limitations, such as the limited number of participating airports. The contractor also identified limitations regarding estimates of the costs and operational effects of implementing various worker screening methods nationwide. For example, the contractor noted that its cost estimates did not include costs associated with operational effects, such as longer wait times for workers, and potentially costly infrastructure modifications, such as construction of roads and shelters to accommodate vehicle screening.

these decisions into airports' existing systems.[35] To address this issue, we have recommended that TSA develop milestones for meeting statutory requirements for, among other things, performance standards for biometric airport access control systems. DHS concurred with this recommendation.

Finally, TSA's efforts to enhance the security of the nation's airports have not been guided by a national strategy that identifies key elements, such as goals, priorities, performance measures, and required resources. To better ensure that airport stakeholders take a unified approach to airport security, we recommended that TSA develop a national strategy that incorporates key characteristics of effective security strategies, such as measurable goals and priorities, to which DHS concurred.

Cybersecurity

DHS Has Made Progress in Strengthening Cybersecurity, but Further Actions are Warranted

Federal law and policy[36] establish DHS as the focal point for efforts to protect our nation's computer-reliant critical infrastructures. Since 2005, we have reported that DHS has not yet fully satisfied its key responsibilities for protecting these critical infrastructures and have made recommendations for DHS to address in key cyberscurity areas, to include the five key areas shown in table 1.

Table 1: Key Cybersecurity Areas Identified by GAO

1.	Bolstering cyber analysis and warning capabilities
2.	Completing actions identified during cyber exercises
3.	Improving cybersecurity of infrastructure control systems
4.	Strengthening DHS's ability to help recover from Internet disruptions
5.	Addressing cyber crime

Source: GAO.

[35]Among other things, the Intelligence Reform and Terrorism Prevention Act of 2004 directed TSA, in consultation with industry representatives, to establish comprehensive technical and operational system requirements and performance standards for the use of biometric identifier technology in airport access control systems. See Pub. L. No. 108-458, § 4011, 118 Stat. 3638, 3712-14 (2004) (codified at 49 U.S.C. § 44903(h)(5)).

[36]These include The Homeland Security Act of 2002, Homeland Security Presidential Directive-7, and the *National Strategy to Secure Cyberspace.*

DHS has since developed and implemented certain capabilities to satisfy aspects of its responsibilities, but the department has not fully implemented our recommendations and, thus, further action needs to be taken to address these areas. For example, in July 2008, we reported[37] that DHS's United States Computer Emergency Readiness Team did not fully address 15 key attributes of cyber analysis and warning capabilities related to four key areas.[38] As a result, we recommended that the department address shortfalls in order to fully establish a national cyber analysis and warning capability. DHS agreed in large part with our recommendation. Similarly, in September 2008, we reported that since conducting a major cyber attack exercise, called Cyber Storm, DHS had demonstrated progress in addressing eight lessons it had learned from these efforts, but its actions to address the lessons had not been fully implemented. [39] Consequently, we recommended that DHS complete corrective activities to strengthen coordination between public and private sector participants in response to significant cyber incidents. DHS concurred with our recommendation and has made progress in completing some identified activities.

We also testified in March 2009 on needed improvements to the nation's cybersecurity strategy.[40] In preparing for that testimony, we obtained the views of experts (by means of panel discussions) on critical aspects of the strategy, including areas for improvement.

The experts, who included former federal officials, academics, and private sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cybersecurity posture. The key strategy improvements identified by these experts are listed in table 2.

[37]GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C.: July 31, 2008).

[38]The four key areas are: (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat.

[39]GAO, *Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned from Its First Cyber Storm Exercise*, GAO-08-825 (Washington, D.C.: Sept. 9, 2008).

[40]GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: Mar.10, 2009).

Table 2: Key Strategy Improvements Identified by Cybersecurity Experts

1.	Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.
2.	Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
3.	Establish a governance structure for strategy implementation.
4.	Publicize and raise awareness about the seriousness of the cybersecurity problem.
5.	Create an accountable, operational cybersecurity organization.
6.	Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7.	Bolster public-private partnerships through an improved value proposition and use of incentives.
8.	Focus greater attention on addressing the global aspects of cyberspace.
9.	Improve law enforcement efforts to address malicious activities in cyberspace.
10.	Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts.
11.	Increase the cadre of cybersecurity professionals.
12.	Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

These recommended improvements to the national strategy are in large part consistent with our previous reports and extensive research in this area. Until they are addressed, our nation's most critical federal and private sector cyber infrastructure remain at unnecessary risk to attack from our adversaries.

Mr. Chairman, this concludes my statement for the record.

GAO Contacts and Staff Acknowledgements

For questions about this statement, please contact Cathleen A. Berrick at 202-512-8777, or berrickc@gao.gov. For further information regarding maritime security issues, please contact Stephen L. Caldwell at 202-512-9610, or caldwells@gao.gov. For further information regarding aviation security issues, please contact Stephen M. Lord at 202-512-4379, or lords@gao.gov. For further information regarding cybersecurity issues, contact David A. Powner at 202-512-9286, or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

Acknowledgments

In addition to the contacts named above, Christopher Conrad, Assistant Director, managed this review. Jonathan Bachman, Dave Bruno, Lisa Canini, Joseph Cruz, Michael Gilmore, Barbara Guffy, Lemuel Jackson,

Steve Morris, Robert Rivas, Yanina Golburt Samuels, and Rebecca Kuhlmann Taylor made significant contributions to the work. Frances Cook, Geoffrey Hamilton, Tom Lombardi, and Jan Montgomery provided legal support. Linda Miller provided assistance in testimony preparation.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548