United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 1:00 p.m. EST
In Camden, New Jersey
Tuesday, December 16, 2003

HOMELAND SECURITY

Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers

Statement of Richard M. Stana, Director
Homeland Security and Justice

December 16, 2003

HOMELAND SECURITY

Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-325T, testimony before the Committee on Energy and Commerce and the Subcommittee on Oversight and Investigations

Why GAO Did This Study

After the attacks of September 11, 2001, concerns intensified that terrorists would attempt to smuggle a weapon of mass destruction into the United States. One possible method for terrorists to smuggle such a weapon is to use one of the 7 million cargo containers that arrive at our nation's seaports each year. The Department of Homeland Security's U.S. Customs and Border Protection (CBP) is responsible for addressing the potential threat posed by the movement of oceangoing cargo containers. Since CBP cannot inspect all arriving cargo containers, it uses a targeting strategy, which includes an automated targeting system. This system targets some containers for inspection based on a perceived level of risk. In this testimony, GAO provides preliminary findings on its assessment of (1) whether CBP's development of its targeting strategy is consistent with recognized key risk management and computer modeling practices and (2) how well the targeting strategy has been implemented at selected seaports around the country.

GAO is completing its assessment and developing recommendations to address strategy development and implementation challenges.

www.gao.gov/cgi-bin/getrpt?GAO-04-325T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Richard M. Stana at (202) 512-8777 or StanaR@gao.gov.

What GAO Found

CBP has taken steps to address the terrorism risks posed by oceangoing cargo containers. These include establishing a National Targeting Center, refining its automated targeting system, instituting a national training program for its personnel that perform targeting, and promulgating regulations to improve the quality and timeliness of data on cargo containers. However, while CBP's strategy incorporates some elements of risk management, it does not include other key elements, such as a comprehensive set of criticality, vulnerability and risk assessments that experts told GAO are necessary to determine risk and the types of responses necessary to mitigate that risk. Also, CBP's targeting system does not include a number of recognized modeling practices, such as subjecting the system to peer review, testing and validation. By incorporating the missing elements of a risk management framework and following certain recognized modeling practices, CBP will be in a better position to protect against terrorist attempts to smuggle weapons of mass destruction into the United States.

CBP faces a number of challenges at the six ports we visited. CBP does not have a national system for reporting and analyzing inspection statistics and the data provided to us by ports were generally not available by risk level, were not uniformly reported, were difficult to interpret, and were incomplete. CBP officials told us they have just implemented a new module for their targeting system, but it is too soon to tell whether it will provide consistent, complete inspection data for analyzing and improving the targeting strategy. In addition, CBP staff that received the national targeting training were not tested or certified to ensure that they had learned the basic skills needed to provide effective targeting. Further, space limitations and safety concerns about inspection equipment constrained the ports in their utilization of screening equipment, which has affected the efficiency of examinations.

A container ship docks at the Miami seaport

Source: Customs and Border Protection, U.S. Department of Homeland Security

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to be here today to participate in this hearing on the security of oceangoing cargo containers. In the aftermath of the terrorist attacks of September 11, 2001, there is heightened concern that terrorists may try to smuggle weapons of mass destruction into a U.S. port using one of the millions of cargo containers that arrive at our nation's seaports each year. If terrorists did so and detonated such a weapon (e.g., a nuclear or radiological explosive device) at a seaport, the incident could cause widespread death and damage to the immediate area, perhaps shut down seaports nationwide, cost the U.S. economy billions of dollars, and seriously hamper international trade.

The Department of Homeland Security and its U.S. Customs and Border Protection (CBP) are responsible for addressing the threat posed by terrorist smuggling of weapons in oceangoing containers. To carry out this responsibility, CBP uses a targeting strategy, which includes a computerized model called the Automated Targeting System, to help select (or "target") containers for additional review and/or inspection. Organizations that are involved in security matters, such as CBP, frequently employ certain risk management practices, including computer modeling, to help them prioritize their activities and use of resources. In essence, risk management is a systematic process to analyze threats, vulnerabilities, and critical assets to better support management decisions.

This statement presents the preliminary results from our latest effort in a series of GAO reports that evaluate CBP's response to the terrorist threat.[1] Based upon our ongoing assessment of CBP's targeting strategy for this subcommittee, I will provide our preliminary findings on (1) whether CBP's development of its targeting strategy is consistent with recognized risk management and computer modeling practices and (2) how well the targeting strategy has been implemented at selected seaports around the country. Our preliminary findings are based on extensive data collection and analysis at CBP, consultations with experts in terrorism and risk management, visits to six seaports, and related interviews with federal and local government and private sector officials responsible for port security and operations. Additional information on our scope and methodology can be found at the end of this statement. Our work focused primarily on the

[1]A listing of relevant GAO reports appears at the end of this statement.

targeting system rather than the sufficiency of inspections at the ports once a container has been targeted.

Summary

While CBP has taken steps to address the terrorism risks posed by oceangoing cargo containers, its targeting strategy neither incorporates all key elements of a risk management framework, nor is it consistent with certain recognized practices associated with modeling. To its credit, CBP established the National Targeting Center to serve as the national focal point for targeting imported cargo and for distributing periodic intelligence alerts to the ports. CBP has refined its targeting system, which was originally designed to identify narcotics contraband, to help identify containers posing potential terrorist threats for possible physical screening and inspection. It also instituted a national training program for its personnel that perform targeting. Further, CBP promulgated regulations aimed at improving the quality and timeliness of transmitted cargo manifest data for use in the targeting system. However, while its strategy incorporates some elements of risk management, CBP has not performed a comprehensive set of threat, criticality, vulnerability and risk assessments that experts said are vital for determining levels of risk for each container and the types of responses necessary to mitigate that risk. Regarding recognized modeling practices, CBP has not subjected the targeting system to external peer review or testing as recommended by the experts we contacted. CBP has a program to randomly select and inspect containers, to compare these results with those generated by the targeting system. However, because the inspections can be waived, randomly selected containers might not be inspected, which limits the usefulness of the program to help improve the targeting system By incorporating the missing elements of a risk management framework and following recognized modeling practices, CBP would have better information to make management decisions related to preventing terrorist from smuggling weapons of mass destruction into the United States.

CBP faces a number of challenges in implementing the targeting strategy at the six ports we visited that could limit the strategy's effectiveness. First, CBP does not have a national system for reporting and analyzing inspection statistics and the data provided to us by ports were generally not readily available by risk level, were not uniformly reported, were difficult to interpret, and were incomplete. CPB officials told us they have just implemented a new module for their targeting system to better collect national data on the results of inspections, but it is too soon to tell whether it will provide consistent, complete inspection data for analyzing and improving the targeting strategy. In addition, CBP staff that received

the national targeting training were not tested or certified to ensure that they had learned the basic skills needed to provide effective targeting. Further, we found that space limitations and safety concerns about inspection equipment constrain the ports in their utilization of screening equipment, which has affected the efficiency of examinations.

Background

Maritime Cargo Containers Are Important and Vulnerable

Cargo containers are an important segment of maritime commerce. Approximately 90 percent of the world's cargo moves by container. Each year, approximately 16 million oceangoing cargo containers enter the U.S. carried aboard thousands of container vessels. In 2002, approximately 7 million containers arrived at U.S seaports, carrying more than 95 percent of the nation's non-North American trade by weight and 75 percent by value. Many experts on terrorism—including those at the Federal Bureau of Investigation and academic, think tank and business organizations—have concluded that the movement of oceangoing cargo containers are vulnerable to some form of terrorist action. A terrorist incident at a seaport, in addition to killing people and causing physical damage, could have serious economic consequences. In a 2002 simulation of a terrorist attack involving cargo containers, every seaport in the United States was shut down, resulting in a loss of $58 billion in revenue to the U.S. economy, including spoilage, loss of sales, and manufacturing slowdowns and halts in production.[2]

CBP Has A Layered Approach to Select and Inspect Cargo Containers

CBP is responsible for preventing terrorists and weapons of mass destruction from entering the United States. As part of its responsibility, it has the mission to address the potential threat posed by the movement of oceangoing containers. To perform this mission, CBP has inspectors at the ports of entry into the United States. While most of the inspectors assigned to seaports perform physical inspections of goods entering the country, some are "targeters"—they review documents and intelligence reports and determine which cargo containers should undergo additional documentary

[2]The consulting firm Booz Allen Hamilton and The Conference Board sponsored the simulation in 2002. In the simulation, representatives from government and industry participated in a scenario involving the discovery and subsequent detonation of radioactive bombs hidden in cargo containers.

reviews and/or physical inspections. These determinations are not just based on concerns about terrorism, but also concerns about illegal narcotics and/or other contraband.

The CBP Commissioner said that the large volume of imports and its limited resources make it impossible to physically inspect all oceangoing containers without disrupting the flow of commerce. The Commissioner also said it is unrealistic to expect that all containers warrant such inspection because each container poses a different level of risk based on a number of factors including the exporter, the transportation providers, and the importer. These concerns led to CBP implementing a layered approach that attempts to focus resources on potentially risky cargo containers while allowing other cargo containers to proceed without disrupting commerce.

As part of its layered approach, CBP employs its Automated Targeting System (ATS) computer model to review documentation on all arriving containers and help select or "target" containers for additional documentary review and/or physical inspection. The ATS was originally designed to help identify illegal narcotics in cargo containers. ATS automatically matches its targeting rules against the manifest and other available data for every arriving container, and assigns a level of risk (i.e., low, medium, high) to each container. At the port level, inspectors use ATS, as well as other data (e.g., intelligence reports), to determine whether to inspect a particular container. In addition, CBP has a program, called the Supply Chain Stratified Examination, which supplements the ATS by randomly selecting additional containers to be physically examined. The results of the random inspection program are to be compared to the results of ATS inspections to improve targeting. If CBP officials decide to inspect a particular container, they might first use equipment such as the Vehicle and Cargo Inspection System (VACIS) that takes a gamma-ray image of the container so inspectors can see any visual anomalies. With or without VACIS, inspectors can open a container and physically examine its contents.

Other components of the layered approach include the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT). CSI is an initiative whereby CBP places staff at designated foreign seaports to work with foreign counterparts to identify and inspect high-risk containers for weapons of mass destruction before they are shipped to the United States. C-TPAT is a cooperative program between CBP and members of the international trade community in which private companies

agree to improve the security of their supply chains in return for a reduced likelihood that their containers will be inspected.[3]

Risk Management and Modeling Are Important Security Practices

Risk management is a systematic process to analyze threats, vulnerabilities, and the criticality (or relative importance) of assets to better support key decisions linking resources with prioritized efforts for results. Risk management is used by many organizations in both government and the private sector. In recent years, we have consistently advocated the use of a risk management approach to help implement and assess responses to various national security and terrorism issues.[4] We have concluded that without a risk management approach that provides insights about the present threat and vulnerabilities as well as the organizational and technical requirements necessary to achieve a program's goals, there is little assurance that programs to combat terrorism are prioritized and properly focused. Risk management could help to more effectively and efficiently prepare defenses against acts of terrorism and other threats. Key elements of a risk management approach are listed below.

- Threat assessment: A threat assessment identifies adverse events that can affect an entity, which may be present at the global, national, or local level.
- Vulnerability assessment: A vulnerability assessment identifies weaknesses in physical structures, personnel protection systems, processes or other areas that may be exploited by terrorists.
- Criticality assessment: A criticality assessment identifies and evaluates an entity's assets or operations based on a variety of factors, including importance of an asset or function.
- Risk assessment: A risk assessment qualitatively and/or quantitatively determines the likelihood of an adverse event occurring and the severity, or impact, of its consequences.

[3]For more information on these programs, see U.S. General Accounting Office, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*, GAO-02-770 (Washington, D.C.: July 2003).

[4]For example, see U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: July 2003).

- Risk characterization: Risk characterization involves designating risk on a scale, for example, low, medium, or high. Risk characterization forms the basis for deciding which actions are best suited to mitigate risk.

- Risk mitigation: Risk mitigation is the implementation of mitigating actions, taking into account risk, costs, and other implementation factors.

- Systems Approach: An integrated systems approach to risk management encompasses taking action in all organizational areas, including personnel, processes, technology, infrastructure, and governance.

- Monitoring and evaluation: Monitoring and evaluation is a continuous repetitive assessment process to keep risk management current and relevant. It includes external peer review, testing, and validation.

Modeling can be an important part of a risk management approach. To assess modeling practices related to ATS, we interviewed terrorism experts and representatives of the international trade community who were familiar with modeling related to terrorism and/or ATS and reviewed relevant literature. There are at least four recognized modeling practices that are applicable to ATS as a decision-support tool.

- Conducting external peer review: External peer review is a process that includes an assessment of the model by independent and qualified external peers. While external peer reviews cannot ensure the success of a model, they can increase the probability of success by improving the technical quality of projects and the credibility of the decision-making process.

- Incorporating additional types of information: To identify documentary inconsistencies, targeting models need to incorporate various types of information to perform complex "linkage" analyses. Using only one type of information will not be sufficient enough to yield reliable targeting results.

- Testing and validating through simulated terrorist events: A model needs to be tested by staging simulated events to validate it as a targeting tool. Simulated events could include "red teams" that devise and deploy tactics in an attempt to define a system's weaknesses, and "blue teams" that devise ways to mitigate the resulting vulnerabilities identified by the red team.

- Using random inspections to supplement targeting: A random selection process can help identify and mitigate residual risk (i.e., the risk remaining after the model-generated inspections have been done), but also help evaluate the performance of the model relative to other approaches.

Positive Steps Taken, But Targeting Strategy Lacks Key Components Of Risk Management And Modeling

CBP has taken several positive steps to address the terrorism risks posed by oceangoing cargo containers. For example, CBP established the National Targeting Center to serve as the national focal point for targeting imported cargo containers and distributing periodic intelligence alerts to the ports. CBP also modified its ATS, which was originally designed to identify narcotics contraband, to include targeting rules for terrorism that could identify high-risk containers for possible physical screening and inspection. In addition, CBP developed a training course for staff responsible for targeting cargo containers. Further, CBP also promulgated regulations aimed at improving the quality and timeliness of transmitted cargo manifest data for use in the targeting system. However, while its strategy incorporates some elements of risk management, CBP has not performed a comprehensive set of threat, criticality, vulnerability and risk assessments that experts said are vital for determining levels of risk for each container and the types of responses necessary to mitigate that risk. Regarding recognized modeling practices, CBP has not subjected ATS to external peer review or testing as recommended by the experts we contacted. Further, CBP has implemented a random inspection designed to improve its targeting rules, but officials at ports can waive the inspections.

CBP Has Taken Several Steps to Improve Its Targeting Strategy

CBP has recognized the potential threat posed by oceangoing cargo containers and has reviewed and updated some aspects of its layered targeting strategy. According to CBP officials, several of the steps that CBP has taken to improve its targeting strategy have resulted in more focused targeting of cargo containers that may hold weapons of mass destruction. CBP officials told us that, given the urgency to take steps to protect against terrorism after the September 11, 2001, terrorist attacks, that they had to take an "implement and amend" approach. That is, they had to immediately implement targeting activities with the knowledge they would have to amend them later. Steps taken by CBP include the following:

- In November 2001, the U.S. Customs Service established the National Targeting Center to serve as the national focal point for targeting imported cargo for inspection.[5] Among other things, the National Targeting Center interacts with the intelligence community and distributes to the ports any intelligence alerts it receives. The National Targeting Center also assists targeters in conducting research on incoming cargo, attempts to improve the targeting of cargo, and manages a national targeting training program for CBP targeters.

- In August 2002, CBP modified the ATS as an anti-terrorism tool by developing terrorism-related targeting rules and implementing them nationally. According to CBP officials responsible for ATS, these targeting rules were developed in consultation with selected intelligence agencies, foreign governments, and companies. CBP is now in the process of enhancing the ATS terrorism-related rules. The newest version of the ATS rules, which is still being tested, gives added risk points when certain rules apply collectively to the same container. CBP refers to this as the "bundling" of rules. In these circumstances, CBP would assume an elevated level of risk for the cargo. Related to this, CBP is currently in the process of developing and implementing further enhancements—known as the "findings module"—to capture additional information related to individual inspections of cargo containers, such as whether an inspection resulted in the discovery of contraband.

- In 2002, CBP also developed a 2-week national training course to train staff in targeting techniques. The course is intended to help ensure that seaport targeters have the necessary knowledge and ability to conduct effective targeting. The course is voluntary and is conducted periodically during the year at the Los Angeles, Long Beach and Miami ports, and soon it will be conducted at the National Targeting Center. In fiscal year 2003, approximately 442 inspectors completed the formal training and CBP plans to train an additional 374 inspectors in fiscal year 2004.

- In February 2003, CBP began enforcing new regulations about cargo manifests—called the "24 hour rule"—which requires the submission of complete and accurate manifest information 24 hours before a

[5]The commercial operations and inspection programs at the U.S. Customs Service (in the Department of the Treasury) were incorporated into CBP (in the new Department of Homeland Security) effective March 1, 2003.

container is loaded on a ship at a foreign port.[6] Penalties for non-compliance can include a CBP order not to load a container on a ship at the port of origin or monetary fines. The rule is intended to improve the quality and timeliness of the manifest information submitted to CBP, which is important because CBP relies extensively on manifest information for targeting. According to CBP officials we contacted, although no formal evaluations have been done, the 24-hour rule is beginning to improve both the quality and timeliness of manifest information. CBP officials acknowledged, however, that although improved, manifest information still is not always accurate or reliable data for targeting purposes.

Targeting Strategy Does Not Incorporate Key Elements of Risk Management

While CBP's targeting strategy incorporates some elements of risk management, our discussions with terrorism experts and our comparison of CBP's targeting system to recognized risk management practices showed that the strategy does not fully incorporate all key elements of a risk management framework. Elements not fully incorporated are discussed below.

- CBP has not performed a comprehensive set of assessments for cargo containers. CBP has attempted to assess the threat of cargo containers through contact with governmental and non-governmental sources. However, it has not assessed the vulnerability of cargo containers to tampering or exploitation throughout the supply chain, nor has it assessed which port assets and operations are the most critical in relation to their mission and function. These assessments, in addition to threat assessments, are needed to understand and identify actions to mitigate risk.

- CBP has not conducted a risk characterization for different forms of cargo, or the different modes of transportation used to import cargo. CBP has made some efforts in this regard by characterizing the risk of each oceangoing cargo containers as either low, medium, or high-risk. But, CBP has not performed a risk characterization to assess the overall risk of cargo containers, or determine how this overall risk characterization of cargo containers compares with sea cargo arriving in other forms, such as bulk cargo (e.g., petroleum and chemical gas

[6]This rule is also known as the Advance Manifest Regulation, 67 Fed. Reg. 66318 (2002). The final regulation was issued October 31, 2002, with implementation beginning February 1, 2003.

shipments) or break-bulk cargo (e.g., steel and wood shipments). Additionally, CBP has not conducted risk characterization to compare the risk of cargo containers arriving by sea with the risk of cargo containers (or other cargo) arriving by other modes, such as truck or rail. These characterizations would enable CBP to better assess and prioritize the risks posed by oceangoing cargo containers and incorporate mitigation activities in an overall strategy.

- CBP actions at the ports to mitigate risk are not part of an integrated systems approach. Risk mitigation encompasses taking action in all organizational areas, including personnel, processes, technology, infrastructure, and governance. An integrated approach would help assure that taking action in one or more areas would not create unintended consequences in another. For example, taking action in the areas of personnel and technology—adding inspectors and scanning equipment at a port—without at the same time ensuring that the port's infrastructure is appropriately reconfigured to accept these additions and their potential impact (e.g., more physical examinations of containers), could add to already crowded conditions at that port and ultimately defeat the purpose of the original actions.

We recognize that CBP implemented the ATS terrorist targeting rules in August 2002 due to the pressing need to utilize a targeting strategy to protect cargo containers against terrorism, and that CBP intends to amend the strategy as necessary. However, implementing a comprehensive risk management framework would help to ensure that information is available to management to make choices about the best use of limited resources. This type of information would help CBP obtain optimal results and would identify potential enhancements that are well-conceived, cost-effective, and work in tandem with other system components. Thus, it is important for CBP to amend its targeting strategy within a risk management framework that takes into account all of the system's components and their vital linkages.

Targeting Strategy Not Consistent With Key Recognized Modeling Practices

Interviews with terrorism experts and representatives from the international trade community who are familiar with CBP's targeting strategy and/or terrorism modeling told us that the ATS is not fully consistent with recognized modeling practices. Challenges exist in each of the four recognized modeling practice areas that these individuals identified: external peer review, incorporating different types of information, testing and validating through simulated events, and using random inspections to supplement targeting.

- With respect to external review, CBP consulted primarily with in-house subject matter experts when developing the ATS rules related to terrorism. CBP officials told us that they considered these consultations to be an extensive process of internal, or governmental, review that helped adapt ATS to meet the terrorist threat. With a few exceptions, CBP did not solicit input from the extended international trade community or from external terrorism and modeling experts.

- With respect to the sources and types of information, ATS relies on the manifest as its principal data input, and CBP does not mandate the transmission of additional types of information before a container's risk level is assigned. Terrorism experts, members of the international trade community, and CBP inspectors at the ports we visited characterized the ship's manifest as one of the least reliable or useful types of information for targeting purposes. In this regard, one expert cautioned that even if ATS were an otherwise competent targeting model, there is no compensating for poor input data. Accordingly, if the input data are poor, the outputs (i.e., the risk assessed targets) are not likely to be of high quality. Another problem with manifests is that shippers can revise them up to 60 days after the arrival of the cargo container. According to CBP officials, about one third of these manifest revisions resulted in higher risk scores by ATS—but by the time these revisions were received, it is possible that the cargo container may have left the port. These problems with manifest data increase the potential value of additional types of information.

- With respect to testing and validation, CBP has not attempted to test and validate ATS through simulated events. The National Targeting Center Director told us that 30 "events" (either real or simulated) are needed to properly test and validate the system. Yet CBP has not conducted such simulations to test and validate the system. Without testing and validation, CBP will not know whether ATS is a statistically valid model and the extent to which it can identify high-risk containers with reasonable assurance. The only two known instances of simulated tests of the targeting system were conducted without CBP's approval or knowledge by the American Broadcast Company (ABC) News in 2002 and 2003. In an attempt to simulate terrorist smuggling highly enriched uranium into the United States, ABC News sealed depleted uranium into a lead-lined pipe that was placed into a suitcase and later put into a cargo container. In both instances, CBP targeted the container that ABC News used to import the uranium, but it did not detect a visual anomaly from the lead-lined pipe using the VACIS and therefore did not open the container.

- With respect to instituting random inspections, CBP has a process to randomly select and examine containers regardless of the risk. The program—the Supply Chain Stratified Examination—measures compliance with trade laws and refocused it to measure border security compliance. One aspect of this new program is random inspections. However, CBP guidance states that port officials may waive the random inspections if available resources are needed to conduct inspections called for by ATS targeting or intelligence tips. Accordingly, although the containers targeted for inspection may be randomly selected, the containers being inspected from the program may not be a random representation. Therefore, CBP may not be able to learn all possible lessons from the program and, by extension, may not be in a position to use the program to improve the ATS rules.

Targeting Strategy Faces Implementation Challenges

Our visits to six seaports found that the implementation of CBP's targeting strategy faces a number of challenges. Specifically, CBP does not have a uniform national system for reporting and analyzing inspection statistics by risk category that could be used for program management and oversight. We also found that the targeters at ports that completed the national training program were not tested and certified, so there is no assurance that they have the necessary skills to perform targeting functions. Further, we found that space limitations and safety concerns constrain the ports in their utilization of screening equipment, which can affect the efficiency of examinations.

CBP Lacks National System To Track Cargo Container Inspections By Risk Category

A CBP official told us that CBP does not have a national system for reporting and analyzing inspection statistics by risk category. While officials at all the ports provided us with inspection data, the data from some ports were generally not available by risk level, were not uniformly reported, were difficult to interpret, and were not complete. In addition, we had to contact ports several times to obtain these data, indicating that basic data on inspections were not readily available. All five ports that gave information on sources of data said they had extracted data from the national Port Tracking System. However, this system did not include information on the number of non-intrusive examinations or physical examinations conducted, according to risk category. Moreover, a CBP headquarters official stated that the data in the Port Tracking System are error prone, including some errors that result from double counting. One port official told us that the Port Tracking System was not suitable for extracting the examination information we had requested, so they had developed a local report to track and report statistics. Our findings are

consistent with a March 2003 Treasury Department Inspector General Report which found, among other things, that inspection results were not documented in a consistent manner among the ports and examination statistics did not accurately reflect inspection activities.[7] A CBP official said that they are in the process of developing a replacement for the Port Tracking System to better capture enforcement statistics but this new system is still in its infancy.

Separately, CBP officials said that they are trying to capture the results of cargo inspections through an enhancement to ATS called the findings module. A National Targeting Center official stated that the findings module would allow for more consistency in capturing standardized inspection results and would also serve as a management control tool. National Targeting Center officials said that the module would be able to categorize examination results according to the level of risk. A CBP official told us the module was being implemented nationwide in late November 2003. While the ATS findings module shows potential as a useful tool for capturing inspection results, it is too soon to tell whether it will provide CBP management with consistent, complete inspection data for analyzing and improving the targeting strategy.

Staff Testing and Certification Could Help Strengthen Targeting Process

While over 400 targeters have completed the new national targeting training, CBP has no mechanism to test or certify their competence. These targeters play a crucial role because they are responsible for making informed decisions about which cargo containers will be inspected and which containers will be released. According to National Targeting Center officials, the goal is for each U.S. seaport to have at least one targeter who has completed national targeting training so that the knowledge and skills gained at the training course can be shared with other targeters at their port of duty. To train other staff, however, the targeter who took the training must have attained a thorough understanding of course contents and their application at the ports. Because the targeters who complete the training are not tested or certified on course materials, CPB has little

[7]Office of Inspector General, Department of the Treasury, *Protecting the Public: Security, Inspection and Targeting of Vessel Containers at U.S. Seaports Can Be Improved*, OIG-03-074, March 28, 2003. This report summarized audit work done at a number of ports during 2001and 2002 on targeting, securing and inspecting cargo containers. The report was done by the Treasury Office of Inspector General because, at that time, inspections were done by the U.S. Customs Service.

assurance that the targeters could perform their duties effectively or that they could train others to perform effectively.

CBP could have better assurance that staff can perform well if CBP tested or certified their proficiency after they have completed the national targeting training. This would also increase the likelihood that course participants are in a position to effectively perform targeting duties and could train others at the ports on how to target potentially suspicious cargo. Further, it would lessen the likelihood that those who did not do well in class are placed in these important positions. Such testing and certification of targeting proficiency would demonstrate CBP's intent to ensure that those responsible for making decisions about whether and how to inspect containers have the knowledge and skills necessary to perform their jobs well.

Space Limitations and Safety Concerns Constrain Use Of Inspection Equipment

One of the key components of the CBP targeting and inspection process is the use of non-intrusive inspection equipment. CBP uses inspection equipment, including VACIS gamma-ray imaging technology, to screen selected cargo containers and to help inspectors decide which containers to further examine. A number of factors constrain the use of non-intrusive inspection equipment, including crowded port terminals, mechanical breakdowns, inclement weather conditions, and the safety concerns of longshoremen at some ports. Some of these constraints, such as space limitations and inclement weather conditions, are difficult if not impossible to avoid.

According to CBP and union officials we contacted, concern about the safety of VACIS is a constraint to using inspection equipment. Union officials representing longshoremen at some ports expressed concerns about the safety of driving cargo containers through the VACIS because it emits gamma rays when taking an image of the inside of the cargo container. Towing cargo containers through a stationary VACIS unit reportedly takes less time and physical space than moving the VACIS equipment over stationary cargo containers that have been staged for inspection purposes. As a result of these continuing safety concerns, some longshoremen are unwilling to drive containers through the VACIS. CBP's response to these longshoremen's concerns has been to stage containers away from the dock, arraying containers in rows at port terminals so that the VACIS can be driven over a group of containers for scanning purposes. However, as seaports and port terminals are often crowded, and there is often limited space to expand operations, it can be space-intensive and time consuming to stage containers. Not all longshoremen's unions have

safety concerns regarding VACIS inspections. For example, at the Port of New York/New Jersey, longshoremen's concerns over the safety of operating the VACIS were addressed after the union contacted a consultant and received assurances about the safety of the equipment. Similar efforts by CBP to convince longshoremen's unions about the safety of VACIS have not been successful at some of the other ports we visited.

In closing, as part of a program to prevent terrorists from smuggling weapons of mass destruction into the United States, CBP has taken a number of positive steps to target cargo containers for inspection. However, we found several aspects of their targeting strategy are not consistent with recognized risk management and modeling practices. CBP faces a number of other challenges in implementing its strategy to identify and inspect suspicious cargo containers. We are now in the process of working with CBP to discuss our preliminary findings and to develop potential recommendations to resolve them. We plan to provide the subcommittee with our final report early next year.

This concludes my statement. I would now be pleased to answer any questions for the subcommittee.

Contacts and Acknowledgments

For further information about this testimony, please contact me at (202) 512-8816. Seto Bagdoyan, Stephen L. Caldwell, Kathi Ebert, Jim Russell, Brian Sklar, Keith Rhodes, and Katherine Davis also made key contributions to this statement.

Appendix: Scope And Methodology

To assess whether the CBP's development of its targeting strategy is consistent with recognized risk management and modeling practices, we compiled a risk management framework and recognized modeling practices, drawn from an extensive review of relevant public and private sector work, prior GAO work on risk management, and our interviews with terrorism experts. We selected these individuals based on their involvement with issues related to terrorism, specifically concerning containerized cargo, the ATS, and modeling. Several of the individuals that we interviewed were referred from within the expert community, while others were chosen from public texts on the record. We did not assess ATS's hardware or software, the quality of the threat assessments that CBP has received from the intelligence community, or the appropriateness or risk weighting of its targeting rules.

To assess how well the targeting strategy has been implemented at selected seaports in the country, we visited various CBP facilities and the Miami, Los Angeles-Long Beach, Philadelphia, New York-New Jersey, New Orleans, and Seattle seaports. These seaports were selected based on the number of cargo containers processed and their geographic dispersion. At these locations, we observed targeting and inspection operations; met with CBP management and inspectors to discuss issues related to targeting and the subsequent physical inspection of containers; and reviewed relevant documents, including training and operational manuals, and statistical reports of targeted and inspected containers. At the seaports, we also met with representatives of shipping lines, operators of private cargo terminals, the local port authorities, and Coast Guard personnel responsible for the ports' physical security. We also met with terrorism experts and representatives from the international trade community to obtain a better understanding of the potential threat posed by cargo containers and possible approaches to countering the threat, such as risk management.

We conducted our work from January to November 2003 in accordance with generally accepted government auditing standards.

Related GAO Products

Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain. GAO-03-1155T. Washington, D.C.: September 9, 2003.

Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors. GAO-03-770. Washington, D.C.: July 25, 2003.

Homeland Security: Challenges Facing the Department of Homeland Security in Balancing its Border Security and Trade Facilitation Missions. GAO-03-902T. Washington, D.C.: June 16, 2003.

Container Security: Current Efforts to Detect Nuclear Material, New Initiatives, and Challenges. GAO-03-297T. Washington, D.C.: November 18, 2002.

Customs Service: Acquisition and Deployment of Radiation Detection Equipment. GAO-03-235T. Washington, D.C.: October 17, 2002.

Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful. GAO-02-993T. Washington, D.C.: August 5, 2002.

Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts. GAO-02-208T. Washington, D.C.: October 31, 2001.

Homeland Security: Key Elements of a Risk Management Approach. GAO-02-150T. Washington, D.C.: October. 12, 2001.

Federal Research: Peer Review Practices at Federal Science Agencies Vary. GAO/RCED-99-99. Washington, D.C.: March 17, 1999.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

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

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548