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 10:00 a.m. EST
Wednesday, March 31, 2004

HOMELAND SECURITY

Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection

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

March 2004

HOMELAND SECURITY

Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-557T, testimony before the Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce

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 is to use one of the 7 million cargo containers that arrive at our seaports each year. Addressing the potential threat posed by the movement of oceangoing cargo containers falls to the Department of Homeland Security's U.S. Customs and Border Protection (CBP). Since CBP cannot inspect all arriving cargo containers, it uses a targeting strategy, including an Automated Targeting System. This system targets containers for inspection based on perceived level of risk. In this testimony, GAO summarizes its work on (1) whether the development of CBP's targeting strategy is consistent with recognized key risk management and modeling practices and (2) how well the strategy has been implemented at selected seaports.

What GAO Recommends

GAO recommends that CBP incorporate all the key elements of a risk management framework and recognized modeling practices in its targeting strategy and the Automated Targeting System. GAO also recommends, among other things, that CBP improve management controls to better implement the targeting strategy at seaports.

The department cited corrective actions taken or planned to address the issues GAO identified.

www.gao.gov/cgi-bin/getrpt?GAO-04-557T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Rich 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, but its strategy neither incorporates all key elements of a risk management framework nor is it entirely consistent with recognized modeling practices. Actions CBP has taken included refining the Automated Targeting System to target cargo containers that are a high risk for terrorism, or other smuggling, for physical inspection. CBP has also implemented national targeting training and sought to improve the quality and timeliness of manifest information, which is one of the inputs for its Automated Targeting System. However, regarding risk management, CPB has not performed a comprehensive set of assessments vital for determining the level of risk for oceangoing cargo containers and the types of responses necessary to mitigate that risk. Regarding recognized modeling practices, CBP has not subjected the Automated Targeting System to adequate external peer review or testing. It has also not fully implemented a process to randomly examine containers in order to test the targeting strategy. Without incorporating all key elements of a risk management framework and recognized modeling practices, CBP cannot be reasonably sure that its targeting strategy provides the best method to protect against weapons of mass destruction entering the United States at its seaports.

GAO's visits to selected seaports found that the implementation of CBP's targeting strategy faces a number of challenges. Although port officials said that inspectors were able to inspect all containers designated by the Automated Targeting System as high-risk, GAO's requests for documentation raised concerns about the adequacy of CBP's data to document these inspections. CBP lacks an adequate mechanism to test or certify the competence of students who participate in their national targeting training. Additionally, CBP has not been able to fully address longshoremen's safety concerns related to inspection equipment. Addressing these concerns is important to ensure that cargo inspections are conducted safely and efficiently. Challenges to both the development and the implementation of CBP's targeting strategy, if not addressed, may limit the effectiveness of targeting as a tool to help ensure homeland security.

A container ship docks at the Miami seaport.

Source: U.S. Customs and Border Protection

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to be here today to provide a summary of our recent report for you on the Department of Homeland Security's (DHS) programs to target oceangoing cargo containers for inspection. This testimony represents a publicly available summary of that report, which DHS designated as Limited Official Use due to the sensitive and specific nature of the information it contains. My prepared statement today also includes appendixes that detail the risk management framework that we developed and the recognized modeling practices that we identified to evaluate DHS's program to target oceangoing cargo containers for inspection.

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.

DHS 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 (e.g., port facilities) to better support management decisions.

This statement presents a summary of 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 a summary of our findings on (1) whether CBP's

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

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 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 targeting system rather than the sufficiency of inspections at the ports once a container has been targeted. We conducted our work from January 2003 to February 2004 in accordance with generally accepted government auditing standards.

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 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. In addition, CBP has a program to augment the targeting strategy by randomly selecting and inspecting containers in order to compare the results of the random inspections with those generated by the targeting system. However, our review disclosed methodological problems with the random inspection program. 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 terrorists 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, and these challenges could limit the strategy's effectiveness. First, we found deficiencies in CBP's national system for reporting and analyzing inspection statistics. CPB officials told us they have just implemented enhancements to 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, we found deficiencies in CBP's national targeting training program. Further, we found that space limitations and safety concerns about inspection equipment constrain some ports in their utilization of screening equipment, a fact that has affected the efficiency of examinations.

Our Limited Official Use report contains several recommendations to DHS on how to better incorporate elements of a risk management framework and recognized modeling practices. Additionally, the report contains recommendations to improve management controls to better implement the targeting strategy at seaports.

DHS provided us with written comments on a draft of our Limited Official Use report. In commenting on that report, DHS stated that in general the report was constructive and that CBP has taken corrective actions and will take further corrective actions to address the issues that we identified. DHS also outlined completion dates to implement these corrective actions.

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. 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 at academic, think tank and business organizations—have concluded that 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 simulated 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 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. Inspectors assigned to seaports help determine which containers entering the country will undergo inspections, and then perform physical inspections of such containers. 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 CBP's 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 scrutiny. The ATS was originally designed to help identify illegal narcotics in cargo containers, but was modified to help identify all types of illegal contraband used by smugglers or terrorists. In addition, CBP has a program, called the Supply Chain Stratified Examination, which supplements ATS by randomly selecting additional containers to be physically examined. The results of the random inspection program are to be compared with the results of ATS inspections to improve targeting. If CBP officials decide to inspect a particular container, they might first conduct a nonintrusive inspection with equipment such as the Vehicle and Cargo Inspection

[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.

System (VACIS), which takes a gamma-ray image of the container so inspectors can detect 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] A supply chain consists of all stages involved in fulfilling a customer request, including stages conducted by manufacturers, suppliers, transporters, retailers, and customers.

Risk Management and Modeling Are Important Security Practices

Risk management is a systematic process to analyze the threats, vulnerabilities, and criticality (or relative importance) of assets in a program to better support key decisions linking resources and program 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 helps to more effectively and efficiently prepare defenses against acts of terrorism and other threats. Key elements of a risk management approach are listed below.

[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).

- Threat assessment: A threat assessment identifies adverse events that can affect an entity, and may be present at the global, national, or local level.

- 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.

- Vulnerability assessment: A vulnerability assessment identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may be exploited by terrorists.

- 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.

- 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.

- Mitigation evaluation: Mitigation evaluation is the identification of mitigating alternatives to assess the effectiveness of the alternatives. The alternatives should be evaluated for their likely effect on the risk and their cost.

- Mitigation selection: Mitigation selection involves a management decision on which mitigation alternatives should be implemented. Selection among alternatives should be based on preconsidered criteria.

- 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 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 Some Key Components of Risk Management and Modeling

CBP Has Taken Several Steps to Improve Its Targeting Strategy

CBP has recognized the potential vulnerability of 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, 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 support its targeting initiatives.[5] Among other things, the National Targeting Center interacts with the intelligence community and manages a national targeting training program for CBP targeters.

- In August 2002, CBP modified the ATS as an antiterrorism tool by developing terrorism-related targeting rules and implementing them nationally. CBP is now in the process of enhancing the ATS terrorism-related rules.

- 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 in the future it will also be conducted at the National Targeting Center.

- 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 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 the timeliness of manifest information submitted to CBP, which is important because CBP relies extensively on manifest

[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.

[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.

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 Some 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 with 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 nongovernmental 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 are the most critical to carrying out its mission—and therefore in the most need of protection. 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. Further, CBP has not performed a risk characterization to assess the overall risk of cargo containers. 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 ensure 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 because of the pressing need to utilize a targeting strategy to protect cargo containers against terrorism, and that CBP intends to amend the strategy as necessary. In doing so, implementing a comprehensive risk management framework would help CBP 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 Fully 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 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 had limited external consultations when developing the ATS rules related to terrorism.

- With respect to the sources and types of information, ATS relies on the manifest as one of its sources of data, and CBP does not mandate the transmission of entry data 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. These problems with manifest data increase the potential value of additional types of information.

- With respect to testing and validation, 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 a terrorist smuggling highly enriched uranium into the United States, ABC News sealed depleted uranium into a lead-lined pipe that was placed in 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 VACIS and therefore did not open the container.

- With respect to instituting random inspections, CBP has a program to randomly select and examine containers regardless of their risk, titled the Supply Chain Stratified Examination. However, our review disclosed methodological problems with this program.

Targeting Strategy Faces Implementation Challenges

CBP Lacks National System to Track Cargo Container Inspections by Risk Category

We found a number of deficiencies in CBP's national system for reporting and analyzing inspection statistics. While officials at all the ports we visited provided us with inspection data, we observed problems with the available data. In addition, we had to contact ports several times to obtain these data, indicating that basic data on inspections were not readily available.

Separately, CBP officials said that they are trying to capture the results of cargo inspections through an enhancement to ATS. These enhancements were not implemented to an extent that we could evaluate their potential effectiveness.

Staff Testing and Certification Could Help Strengthen Targeting Process

CBP does not have an adequate mechanism to test or certify the competence of targeters in their national targeting training program. The targeters taking the training must have 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 assurance that the targeters could perform their duties effectively or that they could train others to perform effectively.

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 nonintrusive inspection equipment. CBP uses nonintrusive 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 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 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 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 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.

Conclusions and Recommendations

One legacy of the September 11, 2001 terrorist attacks is uncertainty. It is unclear if, where, when, and how other attacks might occur and what steps should be taken to best protect national security. In the context of possible smuggling of weapons of mass destruction in cargo containers at our nation's seaports, it is vital that CBP use its resources to maximize the effectiveness of its targeting strategy to reduce this uncertainty. Without incorporating all elements of a risk management framework and utilizing recognized modeling practices, CBP cannot be sure that its targeting

strategy is properly focused and prioritized. In addition, risk management and the use of recognized modeling practices will not ensure security if there are lapses in implementing these practices at the ports. Finally, without instituting a national inspection reporting system, testing and certifying CBP officials that receive the targeting training, and resolving the safety concerns of longshoremen unions, the targeting system's effectiveness as a risk management tool may be limited.

Our Limited Official Use report contains several recommendations to DHS on how to better incorporate key elements of a risk management framework and recognized modeling practices. Additionally, the report contains recommendations to improve management controls to better implement the targeting strategy at seaports.

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, Kathleen Ebert, Jim Russell, and Brian Sklar also made key contributions to this statement. Additional assistance was provided by David Alexander, Katherine Davis, Scott Farrrow, Ann Finley, and Keith Rhodes.

Appendix I: Scope and Methodology

To assess whether CBP's development of its targeting strategy is consistent with recognized risk management and modeling practices, we compiled a risk management framework and a list of 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, 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. We used these statistical reports to determine the type of data available; we did not assess the reliability of the data or use it to make any projections. 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 2003 to February 2004 in accordance with generally accepted government auditing standards.

Appendix II: Risk Management Framework for Homeland Security and Terrorism

Development and Application of Risk Management Framework

This appendix details the risk management framework that GAO developed in order to assess CBP's overall targeting strategy. In recent years, GAO has consistently advocated the use of a risk management approach as an iterative analytical tool to help implement and assess responses to various national security and terrorism issues.[1] We have concluded that without a risk management approach, there is little assurance that programs to combat terrorism are prioritized and properly focused. Risk management principles acknowledge that while risk cannot be eliminated, enhancing protection from known or potential threats can help reduce it. Drawing on this precedent, we compiled a risk management framework—outlined below—to help assess the U.S. government's response to homeland security and terrorism risk. One way in which the Department of Homeland Security's U.S. Customs and Border Protection has already begun to manage risk is by developing and implementing the Automated Targeting System to target high-risk oceangoing containerized cargo for inspection.

Applied to homeland security and terrorism risk, the framework assumes that the principal classes of risk from terrorism are to (1) the general public; (2) organizational, governmental, and societal infrastructure; (3) cyber and physical infrastructure; and (4) economic sectors/structures. Terrorism risk is framed by and is a function of (1) a strategic intent of inflicting extreme damage and disruption; (2) operational, logistical, and technological capabilities including the ability to obtain and deploy various classes of weapons against targets of least resistance (targets are chosen and prioritized according to their attractiveness or utility, based, in turn, on the potential for economic or human loss, their symbolic value, and name recognition); and (3) rational responses to moves designed to counteract them. This last aspect includes the identification and exploitation of loopholes in the response. A principal example of potential homeland security or terrorism risk is the global supply chain, a complex system of multiple interacting components with interdependent risk, and with the potential for this risk to be transferred from any weak links in the chain. The risk posed to the supply chain at the operational, or tactical, level is manifested, for example, in the movement of oceangoing containerized cargo.

[1]U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: October, 31, 2001) and U.S. General Accounting Office, *Key Elements of a Risk Management Approach*, GAO-02-150T (Washington, D.C.: October 12, 2001).

Importance, Benefits, and Limitations of Risk Management

In terms of the importance of risk management, an entity exists to provide value for its stakeholders in an environment of uncertainty, which is a function of the ability to determine the likelihood of events occurring and quantify the resulting outcomes. As applied to homeland security, "value" is realized as protection (security) provided by the U.S. government against terrorism risk at an acceptable cost (function of time and money) for the recipients of the valued service (for example, the general public and the business community). This value might, on occasion, be at risk (worst-case loss scenario) that needs to be managed, thus risk management can be viewed as an integral part of managing homeland security.

In terms of its benefits, risk management enables entities to operate more effectively in environments filled with risks by providing the discipline and structure to address them; risk management is not an end in itself but an important means of an entity's management process. As such, it is interrelated with, among other things, an entity's governance, performance management, and internal control. Further, risk management provides the rigor necessary to identify and select among alternative risk responses whose cumulative effect is intended to reduce risk, and the methodologies and techniques for making selection decisions. Also, risk management enables entities to have an enhanced capability to identify potential events, assess risks, and establish integrated responses to reduce "surprises," and related costs and losses.

In terms of its limitations, ultimately, risk management cannot eliminate risk and the environment of uncertainty that helps sustain it, but risk management can help reduce risk, with a goal of providing reasonable assurance that an entity's objectives will be achieved. Risk management combines elements of science and judgment (human dimension to conflict), and ultimately relies on a set of estimates about risk that lies in the future, which is inherently uncertain. Accordingly, the results of risk management might be called into question because of, among other things, the potential for human errors in judgment and the potentially poor quality of information driving the risk management process.

Risk Management Framework

The framework is a composite of risk management best practices gleaned from our interviews with terrorism and risk-modeling experts and our extensive review of relevant reports on risk management, such as those by GAO, the Congressional Research Service, Booz Allen Hamilton (on contract to the U.S. intelligence community), and the Committee of the

Sponsoring Organizations of the Treadway Commission (in conjunction with PricewaterhouseCoopers).[2]

For purposes of the risk management framework, we used the following definitions:

- ***Risk***—an event that has a potentially negative impact, and the possibility that such an event will occur and adversely affect an entity's assets and activities and operations, as well as the achievement of its mission and strategic objectives. As applied to the homeland security context, risk is most prominently manifested as "catastrophic" or "extreme" events related to terrorism, i.e., those involving more that $1 billion in damage or loss and/or more than 500 casualties.

- ***Risk management***—a continuous process of managing, through a series of mitigating actions that permeate an entity's activities, the likelihood of an adverse event happening and having a negative impact. In general, risk is managed as a portfolio, addressing entity-wide risk within the entire scope of activities. Risk management addresses "inherent," or pre-action, risk (i.e., risk that would exist absent any mitigating action) as well as "residual," or post-action, risk (i.e., the risk that remains even after mitigating actions have been taken).

The risk management framework—which is based on the proposition that a threat to a vulnerable asset results in risk—consists of the following components:

- ***Internal (or implementing) environment***—the internal environment is the institutional "driver" of risk management, serving as the foundation of all elements of the risk management process. The internal environment includes an entity's organizational and management structure and processes that provide the framework to plan, execute, and control and monitor an entity's activities, including risk management. Within the

[2]The framework is adapted from primary sources, including reports by GAO; the Congressional Research Service; Department of Energy's Office of Science and Technology; National Academies/National Research Council; Committee of the Sponsoring Organizations of the Treadway Commission/PricewaterhouseCoopers; Risk Management Solutions, and RiskMetrics (private risk management consulting firms advising insurance, reinsurance, and financial services companies on terrorism and other catastrophic events); Booz Allen Hamilton, on contract to the U.S. government intelligence community; academic and think-tanks (e.g., Brookings Institution, Council on Foreign Relations) papers on responses to terrorism, including risk management; and interviews with terrorism and risk modeling experts.

organizational and management structure, an operational unit that is independent of all other operational (business) units is responsible for implementing the entity's risk management function. This unit is supported by and directly accountable to an entity's senior management. For its part, senior management (1) defines the entity's risk tolerance (i.e., how much risk is an entity willing to assume in order to accomplish its mission and related objectives) and (2) establishes the entity's risk management philosophy and culture (i.e., how an entity's values and attitudes view risk and how its activities and practices are managed to deal with risk). The operational unit (1) designs and implements the entity's risk management process and (2) coordinates internal and external evaluation of the process and helps implement any corrective action.

- ***Threat (event) assessment***—threat is defined as a potential intent to cause harm or damage to an asset (e.g., natural environment, people, man-made infrastructures, and activities and operations). Threat assessments consist of the identification of adverse events that can affect an entity. Threats might be present at the global, national, or local level, and their sources include terrorists and criminal enterprises. Threat information emanates from "open" sources and intelligence (both strategic and tactical). Intelligence information is characterized as "reported" (or raw) and "finished" (fully fused and analyzed).

  As applied to homeland security and terrorism risk, and from the perspective of the source of the threat (for example, a terrorist), beginning with intent (the basis of the threat), adverse event scenarios consist of six stages, as shown in table 1.

Table 1: Adverse Event Scenario Stages

Stage	Description
Intent	The terrorist develops malice and an intent to harm
Target acquisition	The terrorist chooses specific target(s) among assets
Planning	The terrorist researches the targets and various attack options
Preparation	Full commitment stage—the terrorist prepares to launch the attack
Execution	The terrorist carries out the attack
"Grace period"	Depending on the nature and success of the attack, there could be a time lag between the attack and its impact

Source: GAO Analysis

- ***Criticality assessment***—criticality is defined as an asset's relative importance. Criticality assessments identify and evaluate an entity's assets based on a variety of factors, including the importance of its mission or function, the extent to which people are at risk, or the significance of a structure or system in terms of, for example, national security, economic activity, or public safety. Criticality assessments are important because they provide, in combination with the framework's other assessments, the basis for prioritizing which assets require greater or special protection relative to finite resources.

- ***Vulnerability assessment***—vulnerability is defined as the inherent state (either physical, technical, or operational) of an asset that can be exploited by an adversary to cause harm or damage. Vulnerability assessments identify these inherent states and the extent of their susceptibility to exploitation, relative to the existence of any countermeasures. As applied to the global supply chain, a vulnerability assessment might involve, first, establishing a comprehensive understanding of the business and commercial aspects of the chain (as a complex system with multiple interacting participants); and, second, "mapping" the chain and identifying vulnerability points that could be exploited.

- ***Risk assessment***—risk assessment is a qualitative and/or quantitative determination of the likelihood (probability) of occurrence of an adverse event and the severity, or impact, of its consequences. Risk assessments include scenarios under which two or more risks interact creating greater or lesser impacts.

- ***Risk characterization***—risk characterization involves designating risk as, for example, low, medium, or high (other scales, such as numeric, are also be used). Risk characterization is a function of the probability of an adverse event occurring and the severity of its consequences. Risk characterization is the crucial link between assessments of risk and the implementation of mitigation actions, given that not all risks can be addressed because resources are inherently scarce; accordingly, risk characterization forms the basis for deciding which actions are best suited to mitigate the assessed risk.

- **Mitigation evaluation**. Mitigation evaluation is the identification of mitigation alternatives to assess the effectiveness of the alternatives. The alternatives should be evaluated for their likely effect on risk and their cost.

- **Mitigation selection.** Mitigation selection involves a management decision on which mitigation alternatives should be implemented among alternatives, taking into account risk, costs, and the effectiveness of mitigation alternatives. Selection among mitigation alternatives should be based upon preconsidered criteria. There are as of yet no clearly preferred selection criteria, although potential factors might include risk reduction, net benefits, equality of treatment, or other stated values. Mitigation selection does not necessarily involve prioritizing all resources to the highest-risk area, but in attempting to balance overall risk and available resources.

- ***Risk mitigation***—Risk mitigation is the implementation of mitigation actions, in priority order and commensurate with assessed risk; depending on its risk tolerance, an entity may choose not to take any action to mitigate risk (this is characterized as risk acceptance). If the entity does choose to take action, such action falls into three categories: (1) risk avoidance (exiting activities that expose the entity to risk), (2) risk reduction (implementing actions that reduce likelihood or impact of risk), and (3) risk sharing (implementing actions that reduce likelihood or impact by transferring or sharing risk). In each category, the entity implements actions as part of an integrated "systems" approach, with built-in redundancy to help address residual risk (the risk that remains after actions have been implemented). The systems approach consists of taking actions in personnel (e.g., training, deployment), processes (e.g., operational procedures), technology (e.g., software or hardware), infrastructure (e.g., institutional or operational—such as port configurations), and governance (e.g., management and internal control and assurance). In selecting actions, the entity assesses their costs and benefits, where the amount of risk reduction is weighed against the cost involved and identifies potential financing options for the actions chosen.

- ***Monitoring and evaluation of risk mitigation***—Monitoring and evaluation of risk mitigation entails the assessment of the functioning of actions against strategic objectives and performance measures to make necessary changes. Monitoring and evaluation includes, where and when appropriate, peer review and testing and validation; and an evaluation of the impact of the actions on future options; and identification of unintended consequences that, in turn, would need to be mitigated. Monitoring and evaluation helps ensure that the entire risk management process remains current and relevant, and reflects changes in (1) the effectiveness of the actions and (2) the risk environment in which the entity operates—risk is dynamic and threats are adaptive. The risk management process should be repeated periodically, restarting the "loop" of assessment, mitigation, and monitoring and evaluation.

Appendix III: Recognized Modeling Practices Applicable to the Review of ATS

This appendix details the recognized modeling practices that GAO used to assess CBP's computerized targeting model, known as the ATS. CBP characterized ATS as a knowledge, or rule-based, expert system or model that serves as a "decision support tool" in implementing its targeting strategy.[1] Accordingly, for purposes of this report, we identified four practices that are applicable to our review of ATS as such a tool. We identified these practices through our interviews with terrorism experts and representatives of the international trade community—who were familiar with modeling related to terrorism or to ATS—and GAO's chief scientist; and our review of relevant literature, such as reports by the U.S. Department of Energy's Office of Science and Technology and the National Research Council (part of the National Academies)[2] and GAO.[3] The four practices are

- ***Initiating an external peer review of ATS***. Many agencies conduct various types of internal reviews of projects and programs. However, these reviews are usually conducted by managers or supervisors and thus are not independent. Peer review is a process that includes an independent, documented, critical assessment of the technical, scientific merit of research or programs by external peers who are highly qualified scientists with knowledge and expertise equal to that of those whose work they review. In this regard, peers must be capable of making independent judgments about the merit and relevance of what they are reviewing and have no conflicts of interest. If the results are to be used in programmatic decision making, peer reviews can improve the technical quality of projects by recognizing technical weaknesses and suggesting improvements that might be overlooked by those too close to the project;

[1]An expert system is a knowledge collection combined with an inference engine capable of interpreting queries and chaining together separate items of knowledge to develop new inferences; a model is the physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. The knowledge is typically represented as a system of rules or algorithms. An algorithm is a prescribed set of well-defined unambiguous rules or processes for the solution of a problem in a finite number of steps.

[2]The National Academies brings together committees of experts in all areas of scientific and technological endeavor. Four organizations constitute the academies: the National Academy of Sciences, the National Academy of Engineering, the Institute of Medicine, and the National Research Council. The National Research Council was organized by the Academy to associate the broad community of science and technology with the academy's purpose of furthering knowledge and advising the federal government.

[3]U.S. Department of Energy's Office of Science and Technology, *Peer Review in Environmental Technology Development Programs*, (Washington, D.C., 1998); U.S. General Accounting Office, *Federal Research: Peer Review Practices at Federal Science Agencies Vary*, GAO/RCED-99-99 (Washington, D.C.: March 1999).

peer review can also enhance the credibility of the decision-making process by offering frank assessments not constrained by organizational concerns and by avoiding the reality and the perception of conflicts of interest. Peer review cannot ensure the success of a program, but it can increase the probability of success.

- ***Instituting a process of random inspections to supplement targeting***. The experts we spoke with told us that the absence of a process to randomly select containerized cargo for screening or physical examination to supplement ATS was a shortcoming of CBP's targeting strategy. Randomness pertains to a process whose outcome or value depends on chance or on a process that simulates chance, with the implication that all possible outcomes or values have a known, non-zero probability of occurrence—for example, the outcome of flipping a coin or executing a computer-programmed random number generator. A random selection process would not only help mitigate residual risk (i.e., the risk remaining after the original risk mitigation actions have been implemented), but also help evaluate the performance of targeting relative to other approaches.

- ***Enhancing the sources and types of information input into ATS***. Terrorism experts and representatives of the international trade community told us that ATS needed to incorporate additional types of information in order to be able to perform complex "linkage" analyses in an attempt to identify documentary inconsistencies that must be detected to target suspicious containers. They also told us that the ship's manifest (or transportation document that lists a summary of the cargo on board) does not contain enough information in sufficient detail to be useful, by itself, in targeting suspicious containers. These individuals further told us that the movement of containers through the global supply chain generated an additional amount of commercial documentation that could be used for this purpose.[4] Examples of commercial documentation that could be used include purchase orders, commercial invoices, shippers' letters of instruction, and certificates of origin.

- ***Testing and validating ATS by staging simulated terrorist events***. The experts we spoke with emphasized the need to test ATS by

[4]International trade is a tremendously complex business. A typical trade will involve multiple parties—for example, importers, exporters, ocean carriers, financiers, and governments—and may generate 30 to 40 documents.

staging simulated terrorist events in order to validate it as a targeting tool.[5] Simulated events could include "red teams" attempting to smuggle a fake WMD into the United States hidden in an oceangoing cargo container. Red teaming is an approach to "model" a system's adversary and define its weaknesses by devising attack tactics. A blue team may also be used to devise ways to mitigate vulnerabilities in an attempt to defend against the red team. Simulated events would determine whether ATS targeted the suspicious container for screening and/or physical examination, and whether the subsequent screening or examination actually detected the fake WMD.

[5]Validation is the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model or simulation.

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