United States Government Accountability Office

GAO

Report to Congressional Requesters

December 2005

RISK MANAGEMENT

Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure

GAO
Accountability * Integrity * Reliability

G A O

Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-91, a report to Congressional Requesters

December 2005

RISK MANAGEMENT

Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure

Why GAO Did This Study

Congress and the President have called for various homeland security efforts to be based on risk management—a systematic process for assessing threats and taking appropriate steps to deal with them. GAO examined how three Department of Homeland Security components were carrying out this charge:

- the Coast Guard, which has overall responsibility for security in the nation's ports;
- the Office for Domestic Preparedness (ODP), which awards grants for port security projects; and
- the Information Analysis and Infrastructure Protection Directorate (IAIP), which has responsibility for developing ways to assess risks across all types of critical infrastructure.

GAO's work focused on identifying the progress each DHS component has made on risk management and the challenges each faces in moving further.

What GAO Recommends

This report contains many recommendations aimed at helping the three components face their next risk management challenges. DHS, including the Coast Guard, ODP, and IAIP, generally concurred with the report and its recommendations. DHS said that all three components have actions under way to address many of the recommendations in this report.

www.gao.gov/cgi-bin/getrpt?GAO-06-91.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Margaret Wrightson at (415) 904-2200 or wrightsonm@gao.gov.

What GAO Found

The three DHS components GAO studied varied considerably in their progress in developing a sound risk management framework for homeland security responsibilities. The varied progress reflects, among other things, each component's organizational maturity and the complexity of its task (see table below). The Coast Guard, which is furthest along, is the component of longest standing, being created in 1915, while IAIP came into being with the creation of the Department of Homeland Security in 2003. IAIP, which has made the least progress, is not only a new component but also has the most complex task—addressing not just ports but all types of infrastructure. The Coast Guard and ODP have a relatively robust methodology in place for assessing risks at ports; IAIP is still developing its methodology and has had several setbacks in completing the task. All three components, however, have much left to do. In particular, each component is limited in its ability to compare and prioritize risks. The Coast Guard and ODP can do so within a port but not between ports; IAIP has not demonstrated that it can do so either within or between all infrastructure sectors.

Each component faces many challenges in making further progress. Success will depend partly on continuing to improve various technical and management processes that are part of risk management. For example, obtaining better quality data from intelligence agencies would help DHS components estimate the relative likelihood of various types of threats—a key element of assessing risks. In the longer term, progress will depend increasingly on how well risk management is coordinated across agencies, because current approaches in many ways are neither consistent nor comparable. Also, weaving risk-based data into the annual budget cycle of program review will be important. Supplying the necessary guidance and coordination is what the Department of Homeland Security was set up to do and, as the Secretary of Homeland Security has stated, what it now needs increasingly to address. This is a key issue for the department as it seeks to identify relative risks and take appropriate actions related to the nation's homeland security activities.

Progress in Risk Management Is Affected by Organizational Maturity and Complexity of Risk Management Task

DHS component and degree of progress	Organizational characteristics	Complexity of risk management task
Coast Guard: furthest along in developing a risk management framework	Long-standing component; risk management activity began before September 11 attacks	Difficult: must be able to prioritize risks not only within ports but among them
Office for Domestic Preparedness: not as far along, but recent steps are good	Relatively new component transferred from Department of Justice to Department of Homeland Security in 2003	Difficult: for grant purposes, must be able to prioritize risks not only within ports but among them
Information Analysis and Infrastructure Protection Directorate: least far along	New component established with creation of Department of Homeland Security	Extremely difficult: must be able to prioritize risks not only among ports but among all sectors of the nation's critical infrastructure

Source: GAO.

United States Government Accountability Office

Contents

Tables

Figures

Abbreviations

ASME	American Society of Mechanical Engineers
CIP	critical infrastructure protection
COSO	Committee of Sponsoring Organizations
DHS	Department of Homeland Security
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSPD	Homeland Security Presidential Directive
IAIP	Information Analysis and Infrastructure Protection Directorate
IG	Inspector General
MARAD	Maritime Administration
MSRAM	Maritime Security Risk Analysis Model
MTSA	Maritime Transportation Security Act
NADB	National Assets Database
NIPP	National Infrastructure Protection Plan
ODP	Office for Domestic Preparedness
OMB	Office of Management and Budget
PS-RAT	Port Security Risk Assessment Tool
PWCS	Ports, Waterways, and Coastal Security
RAMCAP	Risk Analysis and Management for Critical Asset Protection
TSA	Transportation Security Administration

GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

December 15, 2005

The Honorable Henry A. Waxman
Ranking Minority Member
Committee on Government Reform
House of Representatives

The Honorable C. A. Dutch Ruppersberger
House of Representatives

The threat of terrorism presents a number of risks to our nation's seaports and other types of critical infrastructure. The Department of Homeland Security (DHS) has three components responsible for the security of critical infrastructure related to ports and other facilities. The U.S. Coast Guard has responsibility for port security overall. The Office for Domestic Preparedness (ODP) is responsible for providing port security grants to selected maritime facility owners. The Information Analysis and Infrastructure Protection (IAIP) Directorate is responsible for working with other federal, state, local, and private organizations to identify and protect critical infrastructure across the nation. Risk management is a tool for assessing risks, evaluating alternatives, making decisions, and implementing and monitoring protective measures. This report provides an evaluation of the progress made, and challenges faced, by the Coast Guard, ODP, and IAIP in using risk management to improve homeland security.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will provide copies of this report to appropriate departments and interested congressional committees. This report will also be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (415) 904-2200 or at wrightsonm@gao.gov. Key contributors to this report are listed in appendix III.

Sincerely yours,

Margaret T. Wrightson

Margaret T. Wrightson
Director, Homeland Security and Justice Issues

Executive Summary

Risk management, a strategy for helping policymakers make decisions about assessing risks, allocating resources, and taking actions under conditions of uncertainty, has been endorsed by Congress and the President as a way to strengthen the nation against possible terrorist attacks. Risk management has long been used in such areas as insurance and finance, but its application to domestic terrorism has no precedent. Unlike storms and accidents, terrorism involves an adversary with deliberate intent to destroy, and the probabilities and consequences of a terrorist act are poorly understood and difficult to predict. The size and complexity of homeland security activities and the number of organizations involved—both public and private—add another degree of difficulty to the task. The task of managing this complexity centers on the Department of Homeland Security, which since its inception in March 2003 has been faced with the challenge of transforming 22 agencies into an organization that can plan, manage, and carry out operations effectively. Congress likewise has a key oversight role to play in ensuring that DHS's course regarding risk management reflects a consensus as to the most prudent and cost-effective course of action.

To assist Congress in its oversight, this report focuses on the progress made by three DHS components in applying risk management to homeland security activities and the challenges each component faces in moving further ahead. For two of these components, GAO's review dealt specifically with their risk management activities at the nation's seaports, while the review for the third component encompassed a wider range of infrastructure. GAO decided to focus a considerable amount of this review on seaport security because seaports have been viewed as potential terrorist targets or as conduits for importing a weapon of mass destruction or where terrorists may enter the country. GAO's focus on these three components, while not a comprehensive look across the entire department, provides perspective on the degree of progress made thus far. Risk management has applications for deliberate acts of terror as well as natural disasters, such as hurricanes and earthquakes. GAO's research, which was conducted prior to Hurricane Katrina, focused on preparations for terrorist attacks, not natural disasters. The three components GAO studied are:

- the Coast Guard, the lead federal agency for port security and the agency responsible for developing and coordinating various risk-based assessments of critical infrastructure in and around ports;
- the Office for Domestic Preparedness, administrator of the port security grant program, has awarded more than half a billion dollars in

federal grants to owners and operators of port facilities and vessels; and

- the Information Analysis and Infrastructure Protection Directorate, which has been charged with establishing uniform policies, approaches, guidelines, and methodologies for integrating infrastructure protection and risk management activities within and across key sectors, such as energy, defense, and transportation, including airports, railroads, and ports.[1]

Besides describing the progress of and challenges for each component, this report also presents GAO's observations about what the three components' efforts indicate collectively, both with regard to how far the department has come in managing homeland security efforts on the basis of risk and what steps could help advance the current level of progress.

Background

Seaport security receives particular attention in this report because seaports are widely viewed as representing attractive terrorist targets, in part because of their importance to the economy. More than 95 percent of the nation's non-North American foreign trade (and 100 percent of certain commodities, such as foreign oil) arrives by ship. The estimated economic consequences of a successful attack and resulting shutdown of this system total billions of dollars. Ports also represent attractive targets because they contain a myriad of vulnerabilities. In all, the nation's 300-plus ports have about 3,700 cargo and passenger terminals. Chemical factories, oil refineries, power plants, and other facilities are often located in port areas and add another set of possible targets. Roads crisscross many ports, allowing access by land as well as by water, and the number of people working in or traveling through ports is in the millions. The Coast Guard has the major responsibility for seaport security, and the port security grant program administered by ODP adds to the resources available for port security projects.

Relative to the Coast Guard and ODP, IAIP's homeland security responsibilities are by far the widest-ranging. The Homeland Security Act

[1] On November 14, 2005, DHS reorganized the department. ODP and the Infrastructure Protection part of the former IAIP Directorate are now components in the Preparedness Directorate. We recognize the recent organizational changes, but because ODP and IAIP carried out the work we reviewed, we have not changed the name or organizational posture of these DHS components in our report.

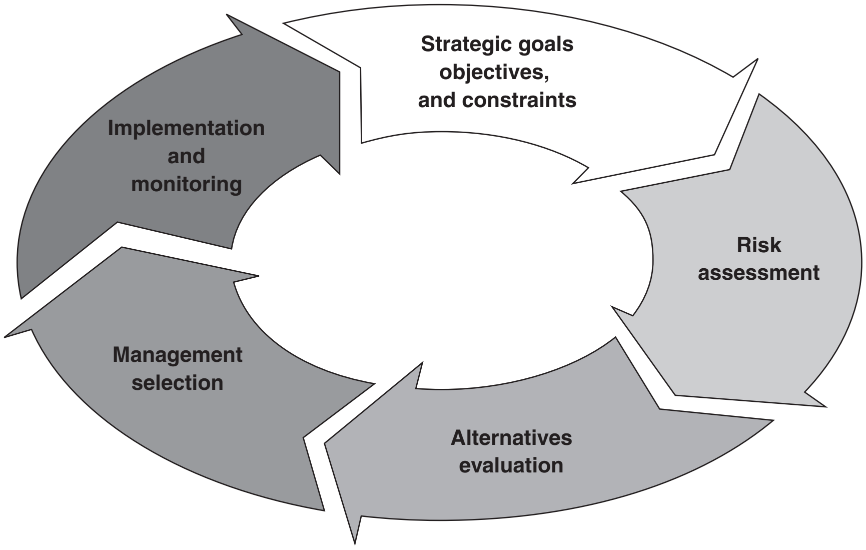
of 2002 and Homeland Security Presidential Directive 7 (HSPD-7) charge IAIP with establishing a risk management framework across the federal government to protect the nation's critical infrastructure and key resources.[2] The scope of this effort is immense, and the effort is one of IAIP's central responsibilities. IAIP's task ultimately involves developing an approach that can inform decisions on what the nation's antiterrorism priorities should be and identifying what strategies and programs will do the most good. IAIP's work is done in a setting where numerous and substantial gaps in security remain, but resources for closing these gaps are limited. More specifically, IAIP is charged with examining and comparing relative risks associated with a multitude of possible targets, ranging from specific structures (such as dams, chemical plants, and nuclear power plants) to major sectors of national infrastructure (such as the banking system, computer networks, and water systems). IAIP is also responsible for developing policies and guidance that other agencies can use in conducting their own risk assessments.

While federal law and the presidential directive call for the use of risk management in homeland security, little specific federal guidance or direction exists as to how risk management should be implemented. To provide a basis for analyzing component efforts, GAO developed a framework for risk management based on industry best practices and other criteria. This framework, shown in figure 1, divides risk management into five major phases: (1) setting strategic goals and objectives, and determining constraints; (2) assessing the risks; (3) evaluating alternatives for addressing these risks; (4) selecting the appropriate alternatives; and (5) implementing the alternatives and monitoring the progress made and results achieved. For all three components, GAO applied this framework after conducting a wide range of interviews with officials, reviewing plans and activities of the three components, and visiting port locations. As part of our work, GAO briefed officials of the three components about the various phases of the framework and the officials generally agreed with its structure and intent. The application of risk management to homeland

[2] The Homeland Security Act incorporates the definition of "critical infrastructure" used in the USA PATRIOT Act of 2001, meaning "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The Homeland Security Act defines "key resources" as "publicly or privately controlled resources essential to the minimal operations of the economy and government." 6 U.S.C. § 101.

security is relatively new, and the framework will likely evolve as processes mature and lessons are learned.

Figure 1: Risk Management Framework



Source: GAO.

Results in Brief

Of the three components GAO reviewed, the Coast Guard had made the most progress in establishing a foundation for using a risk management approach; its next challenges are to further refine and enhance its approach. While the Coast Guard has made progress in all five risk management phases, its greatest progress has been made in conducting risk assessments—that is, evaluating individual threats, the degree of vulnerability, and the consequences of a successful attack. However, the assessments are limited in their reliability and completeness, and better coordination will be needed with the intelligence community so that analysts can develop models that better assess the relative probability of various threat scenarios. The Coast Guard has developed the ability to compare and prioritize risks at individual. However, it cannot yet compare and prioritize relative risks of various infrastructure across ports. Other challenges include developing performance measures to go along with the more general goals already developed for the port security mission, further integrating risk into the annual cycle of program and budget review, and developing formal policies for reviewing and improving the implementation of a risk management approach. The Coast Guard has actions under way to address the challenges it faces in each risk management phase. Several of these actions are based, in part, on briefings GAO held with agency officials.

ODP has made progress in applying risk management to the port security grant program, but like the Coast Guard, it also faces challenges across all phases of the risk management framework. For example, ODP has set broad risk management goals and has placed more emphasis on using risk-based data in its assessments, but it lacks performance measures showing what specific outcomes the program aims to achieve, and it still faces challenges in such matters as comparing grant applications across ports. The grant awards for fiscal year 2004 also illustrate some of the challenges in ensuring that criteria for making the awards are transparent and consistent. At the end of what was, in part, a risk-based assessment process, ODP changed the criteria for awarding grants when it decided to give lower priority to applicants from large companies on the assumption that the companies were better able than other entities to pay for their own improvements. This changed 40 percent of the grants awarded, as projects with higher risk but greater potential for self-funding gave way to lower-risk projects with more limited funding prospects. In the procedures for fiscal year 2005 awards, ODP clarified the criteria it would use in making the awards.

IAIP, which has the broadest risk management responsibilities of the three components and faces the greatest challenges, has made the least progress in carrying out its complex risk management activities. Its efforts are aligned with high-level strategic goals, but ways to measure performance in achieving these goals have yet to be developed. IAIP is not as far along as ODP and the Coast Guard in conducting risk assessments. While IAIP has provided input to ODP for its risk assessment efforts, IAIP's risk assessment responsibilities span much broader sectors of the nation's infrastructure than seaports alone, making its assessment activities more difficult. This difficulty is reflected in the limited progress made. With regard to its risk assessment responsibilities, IAIP has yet to successfully (1) develop data to determine the relative likelihood of various threat scenarios, (2) complete a methodology for comparing and prioritizing key assets, or (3) meet requirements set forth in HSPD-7 for issuing policies and guidance that other agencies can use in conducting their own risk assessments. For example, a DHS consultant issued a risk assessment methodology in 2004 for collecting data from industry, but adverse comments from reviewers have led to revisions that are still under way. IAIP is also challenged in its ability to translate these assessments into specific measures to be taken, because after IAIP makes decisions about what national priorities should be, it is dependent on the actions of others to carry them out. This is particularly true with regard to private sector assets where IAIP needs collaboration from the owners and operators of private sector infrastructure and their regulators.

GAO made four main observations regarding the experience of these three components.

- A considerable degree of effort has been expended thus far, but much work remains to be done. This is particularly true in viewing risk management strategically—that is, with a view that goes beyond just assessing what the risks are and also integrating the consideration of risk into the annual cycle of program and budget review that is already in place.

- The varying degree of progress among the three components tends to reflect several characteristics of each component—how long it has been at the task of developing a risk management approach, how long it has existed as a component and is therefore able to function maturely, and how complex its risk management task is. For example, IAIP, which has made the least progress, is not only a new component established in 2003, but also has the most complex risk-related tasks of the three components—addressing risk not only at ports, but across all types of infrastructure and with multiple federal agencies and nonfederal stakeholders.

- In the near term, all three components' success in risk management will depend partly on continuing to make progress on the challenges described above. This involves continuing to work on such matters as performance measures, basic policies, and enhancements to existing risk assessment tools.

- The final observation is related to a critical longer-term need: more guidance and coordination from the department level, both to help ensure that individual components such as IAIP are carrying out their roles effectively and to ensure that the various responses from individual components mesh as effectively as possible with one another. In comparing the approaches developed by the three components, GAO noted ways in which their efforts were not consistent. The danger is that if components develop systems and methodologies that are inconsistent, they may end up with incompatible systems that have little or no ability to inform spending decisions on homeland security. The challenges associated with creating a department that can effectively administer a coherent risk management approach to the nation's homeland security have been widely acknowledged. IAIP recognizes that as DHS's individual components begin to mature in their risk management efforts, the need increases for ensuring consistency and coherence in these efforts. Supplying this necessary guidance and coordination is what DHS was set up to do.

Principal Findings

Coast Guard Has Made Progress in Using Risk Management, but Challenges Remain

The Coast Guard has made progress across all five phases of risk management. In the first phase (goal and objective setting), the Coast Guard has established broad strategic goals for port security, including, in order of priority: (1) preventing terrorist attacks within, and terrorist exploitation of, the maritime domain and (2) reducing America's vulnerability to terrorism in the maritime domain. It faces challenges in developing objectives that translate these goals into more specific and measurable results. Coast Guard officials recognize that developing performance measures is a necessary next step and have actions under way to develop such measures.

For the second phase, assessing risks, the Coast Guard has greatly expanded the scope of its risk assessment activities since the terrorist attacks of September 11, 2001. It has conducted three major security assessments at the port level, and collectively these assessments have resulted in considerable progress in understanding and prioritizing risks within a port. After it initiated port-level assessments, the Coast Guard expanded its analysis efforts to the national level to gain a more strategic perspective on port security. In all, the Coast Guard has conducted three major efforts at the national level, focusing more generally on understanding the risk posed to various classes of assets (such as bridges or container ships) by various types of attacks (such as using explosives or weapons of mass destruction). The assessments are limited in their reliability and completeness, however, in the degree to which the Coast Guard has (1) formal and systematic input from the intelligence community for modeling relative probability and likelihood of threat scenarios and (2) risk assessment tools allowing comparison and prioritization of specific infrastructure across ports. These limitations affect the degree to which the Coast Guard is able to determine how best to focus its attention on these threats that, from a national perspective, pose the greatest risk within the seaport sector. The Coast Guard has initiated actions to address these challenges. For example, the agency has initiated contact with the intelligence community to obtain better data on threat scenarios, and it plans to complete development of an assessment tool that will compare the relative risks of high-value assets at one port with risks of assets in a different port.

Enhancing these first two phases of risk management is key to making additional progress on the next two phases—evaluating and selecting alternatives that reduce risk. While the Coast Guard's efforts have resulted in progress in identifying and evaluating alternatives at the individual port level, the lack of measurable objectives and sufficient information to fully depict threats, vulnerabilities, and consequences limits the ability to target the areas with the greatest gaps or produce the most cost-effective decisions. Similarly, buttressing annual budget review cycles with risk-based data is in its early development and more work remains to be done. Finally, with regard to the fifth phase—implementation and monitoring—the Coast Guard has implemented a number of activities to mitigate risks and has demonstrated the ability to evaluate its efforts and make improvements. The actions taken have included establishing maritime intelligence centers on the Atlantic and Pacific coasts and working closely with nonfederal stakeholders to reduce vulnerabilities in and around facilities and vessels. However, existing feedback mechanisms are insufficient to ensure that Coast Guard field personnel can make their headquarters managers aware of ways to improve the process. The Coast Guard recognizes the value of formal feedback loops as a means of improving its risk management processes, and it has plans to obtain formal feedback as part of its future efforts.

ODP's Port Security Grant Program Illustrates Both Progress and Challenges in Implementing Risk Management

Like the Coast Guard, ODP has made progress across all five phases of risk management. For example, for the first phase, it has set risk management goals that support broader maritime goals, such as protecting critical infrastructure in harbors, borders, ports, and coastal approaches. ODP has not begun to translate these broad goals into measurable objectives. Without them, it is difficult to know what progress has been made in reducing risk and what security gaps remain.

ODP has carried out risk assessments, with input from the Coast Guard and IAIP, and evaluated mitigation alternatives—the second and third phases of the framework—to help determine which ports should receive priority for grants. Using risk assessments, ODP narrowed the number of ports eligible for grants from 129 to 66 for fiscal year 2005. Other recent steps include placing greater emphasis on using threat, vulnerability, and consequence data in prioritizing grant applications. Along with this progress, however, are several methodological challenges that limit such things as the usefulness of data received from intelligence agencies and ODP's ability to compare and prioritize risks among ports. For example, without data on the relative probability of various threat scenarios from the Coast Guard or IAIP, ODP may not target the most significant security needs. ODP has not yet developed approaches for addressing most of these challenges.

While ODP has also made progress in developing a risk-based grant selection process and mechanisms to monitor what the grants accomplish, grant awards for fiscal year 2004 illustrate the challenges involved in actually making risk-based decisions. At the end of its process for determining which grants to fund, based in part on risk, ODP decided to give lower priority to grants involving projects at large companies, on the assumption that the companies were better able than other entities to pay for their own improvements. For example, one chemical company's application for $225,000 to purchase cameras, fencing, and barricades was initially ranked 25th out of 287 applications nationwide, but under the revised priorities its ranking fell to 236th. Projects initially ranked much lower received funding instead. For example, an application initially ranked as 279th out of 287 was approved for funding. In all, the application of non-risk criteria changed 40 percent of the grants awarded. ODP's changes affected the transparency and consistency of the awards process, in that (1) the criteria under which applications were submitted and initially considered were changed at the end of the process, and (2) the role of risk in evaluating the applications was obscured, because the resulting awards may not have addressed the most severe security gaps. Additionally, there is no guarantee that large companies would spend their own funds for security improvements, and it is unclear whether there are incentives, such as minimum standards for security, that would motivate them to do so. ODP issued revised criteria for fiscal year 2005 grants, and in doing so has made the process more transparent and consistent.

IAIP's Progress in Carrying Out Risk Management Has Been Limited

IAIP's progress in all five phases of risk management has been limited. It has made some progress in developing goals, having issued an Interim National Infrastructure Protection Plan in February 2005 that identifies a strategy for identifying, prioritizing, and coordinating the protection of critical infrastructure and key resources.[3] The interim plan provides some

[3] In November 2005, DHS issued a revised Interim National Infrastructure Protection Plan for comment.

guidance in meeting IAIP's broad responsibilities for identifying, comparing, and prioritizing critical assets, but it is not a comprehensive document, and IAIP faces several challenges in making it more comprehensive. These challenges are related to (1) developing performance measures that can be used in evaluating progress and (2) establishing milestones and time frames for processing and prioritizing assets across the many different infrastructure sectors.

IAIP's progress in risk assessment—the second phase of risk management—has been limited in several main respects. For example, IAIP has experienced difficulties in carrying out requirements of the Homeland Security Act of 2002 that charged IAIP with the responsibility of conducting risk assessments of critical infrastructure and key resources to determine the risks of particular types of terrorist attacks. IAIP's original methodology for this task, called the Risk Analysis and Management for Critical Asset Protection, required extensive modification after its initial issuance in April 2004. IAIP now views it as a tool for engaging industry in a risk management dialogue with government. In September 2005, IAIP officials said they are developing a National Comparative Risk Assessment to meet the immediate need of examining risks within and across sectors, and they plan to complete an interim assessment by the end of 2006. Challenges to carrying out this timetable include the need to obtain key information from other federal agencies and the fact that IAIP still needs to award the contract for this effort. One specific issue is the approach IAIP has taken in assessing the probability of various threat scenarios. The Homeland Security Act calls on IAIP to assess the probability of success of terrorist attacks, and during the course of GAO's review, IAIP officials said they recognize the importance of assessing the relative likelihood of an attack in meeting this requirement. IAIP officials said that the lack of intelligence analysis and data on such things as the capability and intent of terrorist groups hinders their ability to assess probability, but that work is under way in this regard. IAIP officials also pointed out that some inaccuracy is to be expected in examining the intent and capability of an adversary whose plans are concealed and that it will be important to reduce the potential of low-confidence assessments having undue influence when long-term investment decisions are made.

IAIP's progress in the three other phases of risk management (evaluating alternatives, selecting a solution, and implementing and monitoring that solution) will remain limited, in part because of the points just discussed—performance goals and a complete risk assessment methodology are not in place. Beyond these limitations, however, IAIP faces additional challenges. For example, IAIP's role in selection, implementation, and monitoring is further complicated because in many instances, other entities have primary responsibility for selecting the solution. For example, other agencies, such as the Department of Defense or the Department of Energy, have primary responsibilities for some of the infrastructure sectors covered in IAIP's assessments. Additionally, much of the critical infrastructure is owned or operated by private industry, and while IAIP does not have authority over them, other federal agencies do have authority over infrastructure in specific sectors. This condition highlights the importance of coordination between IAIP and agencies with such regulatory authority. For example, the Nuclear Regulatory Commission, which issues licenses to nuclear power plants, has regulatory authority over security matters at these facilities. IAIP officials said they use their expertise and powers of persuasion to bring about specific actions but in most cases cannot compel others to adopt IAIP's recommendations.

Overall Observations

A great amount of effort has been applied. However, much more remains to be done than has been accomplished so far. Across all three components, the most progress has generally been made on fundamental steps, such as conducting risk assessments of individual assets, and less progress has generally been made on developing ways to translate this information into comparisons and priorities across ports and across infrastructure sectors, or applying it to new programs. Progress among the three components' efforts has been far from consistent and has tended to vary not only with the length of time the component has been using a risk-based approach, but also with the component's own maturity level and the complexity of its risk management task.

With regard to next steps that would appear to add the most value to making further progress, one key observation is that in the short term, progress is heavily dependent on continuing to improve basic policies, procedures, and methods for applying risk management. Each component has an admittedly difficult set of challenges ahead, but progress has to be built on taking these incremental steps and doing them well. An area that needs further attention by all three entities is working with intelligence communities to develop improved analysis and data so that the relative probability of various threat scenarios can be further developed.

The final observation is that in the longer term, progress will become increasingly dependent on how well the entire risk management effort is coordinated. While absolute compatibility among all components' efforts is likely impossible, even with components working in close cooperation, strong coordination is important to help ensure that component efforts are consistent rather than stovepiped. The risk management efforts GAO examined appeared to be fueled by a strong concern to make some headway, with coordination and interagency consistency a lesser concern. For example, the Coast Guard initiated efforts to set up a methodology for assessing and specifying risks before IAIP was created; and in the view of IAIP officials, it was important to proceed even though they recognized that doing so might lead to approaches that would not mesh cleanly with the approach IAIP would eventually develop. That approach appeared prudent in the short term, in that if the Coast Guard had waited to begin until guidelines had been set, it would still be waiting. Now, however, the need for coordination is looming larger, and coordination is essential to the success of efforts over time. Some of this coordination needs to come from IAIP, which is required under presidential directive to issue guidelines for other agencies to use, but it has yet to do so. Beyond IAIP, DHS has an active role in this regard. This is a key issue for the department as it moves from being an organization that is essentially in its early stages to one that is increasingly being expected to respond in a way that is more organizationally mature. Since 2003, GAO has designated the implementation and transformation of DHS as high risk because of the numerous challenges in transforming 22 agencies into one department and the serious implications of failure. Translating the concept of risk management into applications that are consistent and useful represents one of these challenges, and failure to effectively address this could have serious consequences for homeland security. In risk management, which the department has embraced as the guiding principle behind its policies and operations, IAIP's role is to act as an intra-agency and interagency coordinator of homeland security activities. Doing so will strengthen its ability to weigh risks and inform the decisions made across the homeland security responsibilities of the many agencies involved.

Recommendations for Executive Action

GAO is making a number of specific recommendations to the Secretary of DHS with regard to the challenges faced by the three components. These recommendations, listed specifically at the end of the relevant chapters, cover such matters as developing performance goals and measures, improving risk assessment methodologies, working with intelligence communities to develop better data for risk assessment purposes, and (for IAIP) developing guidance for other agencies to use in evaluating risk and considering risk mitigation alternatives.

Agency Comments and Our Evaluation

We provided DHS a draft of this report for its review and comment. DHS, including the Coast Guard, ODP, and IAIP, generally agreed with our findings and recommendations. For instance, DHS said that each DHS component we reviewed has actions under way to address recommendations made in the report. The comments from each component are summarized at the end of the relevant chapters. In addition to commenting on our findings and recommendations, DHS provided technical comments under separate cover, and we revised the draft report where appropriate. Written comments from DHS are reprinted in appendix II.

Chapter 1: Introduction: Risk Management Is a Key Tool for Homeland Security

This is a report about the nation's progress in applying risk management to key aspects of homeland security. Risk management is a widely endorsed strategy for helping policymakers make decisions about allocating finite resources and taking actions in conditions of uncertainty. It has been widely practiced for years in such areas as insurance, construction, and finance. By comparison, its application in homeland security is relatively new—much of it coming in the wake of the terrorist attacks of September 11—and it is a difficult task with little precedent. The goals for using it in homeland security include informing strategic decisions on ways to reduce the likelihood that adverse events will occur, and mitigate the negative impacts of and ensure a speedy recovery from those that do. Achieving these goals involves making policy decisions about what the nation's homeland security priorities should be—for example what the relative security priorities should be among seaports, airports, and rail—and basing spending decisions on what approaches or strategies will do the most good at narrowing the security gaps that exist. Risk management has been widely supported by the President and Congress as a management approach for homeland security, and the Secretary of the Department of Homeland Security has made it the centerpiece of agency policy.

"Homeland security" is a broad term with connotations that resonate from the September 11 attacks and other connotations that now resonate from the disaster brought on by Hurricane Katrina in August 2005. Risk management has applications for deliberate assaults like the September 11 attacks and natural disasters, such as hurricanes and earthquakes. Our research was completed and the report largely written before Hurricane Katrina struck. Thus, our work concentrated on components' actions in response to terrorism.

This report examines how three DHS components have applied risk management to certain aspects of their homeland security responsibilities. The three components are the United States Coast Guard, the Office for Domestic Preparedness, and the Information Analysis and Infrastructure Protection Directorate. This report looks at risk management efforts of the Coast Guard and ODP specifically related to seaport security, and for IAIP, it looks at risk management efforts related to IAIP's broader responsibilities in assessing terrorist threats against all aspects of the nation's infrastructure.[1]

Risk Management Has a Long History of Use in Industry and Government

Risk management can be described as the continuous process of assessing risks, reducing the potential that an adverse event will occur, and putting steps in place to deal with any event that does occur.[2] It has been used in the private and public sectors for decades (see table 1 for examples). For example, insurance companies use a variety of statistical techniques to assess the level of risk for what they are insuring. Within government, agencies use risk management to set regulations and to protect the environment and the health and safety of American taxpayers. Although some risk management methodologies and processes can be complex and may require expert advice and support, other aspects of risk management—such as setting goals and using performance measures to track progress in meeting them—are well understood and widely practiced.

[1] On November 14, 2005, DHS reorganized the department. ODP and the Infrastructure Protection component of the former IAIP Directorate are now in the Preparedness Directorate. We recognize the recent organizational changes, but because ODP and IAIP carried out the work we reviewed, we have not changed the name or organizational posture of these DHS components in our report.

[2] A more precise description of risk management is that it involves a continuous process of managing—through a series of mitigating actions that permeate an entity's activities—the likelihood of an adverse event and its negative impact. Risk management addresses risk before mitigating action, as well as the risk that remains after countermeasures have been taken. A glossary of risk management terms is contained at the end of appendix I.

Table 1: Examples of Risk Management in the Private and Public Sectors

Type of application	How risk management is used
Private sector examples	
Insurance	Insurance companies evaluate risks when insuring businesses and homeowners against natural disasters. They assess the probability of natural disasters, such as hurricanes and earthquakes, based on past history and the costs resulting from the damage caused or the lives lost. On the basis of analysis such as this, companies set policies and costs that apply to businesses and homeowners.
Engineering	Engineering firms have analyzed risks related to safety and security when designing chemical plants, nuclear reactors, or bridges. Using risk analysis techniques, they examine the possible threats to the safety and security of the structure and evaluate ways to address the threat by considering various design features that could reduce vulnerabilities or consequences. One example is designing double-hulled oil tankers to reduce the risk of an Exxon Valdez type oil spill.
Banking and finance	Banks and financial institutions assess risks associated with various investment options. For example, spending funds on overseas investments could involve assessing political, social, and financial risks as well as the potential market share that could be gained. Assessments such as these inform decisions on where and whether capital should be invested.
Public sector examples	
Food and Drug Administration	The Food and Drug Administration assesses risk associated with diseases related to various types of food. It examines whether diseases are linked to types of fish and dairy goods. It examines the types and costs of health problems that may occur and it recommends and sets policies or regulations aimed at improving food safety.
Environmental Protection Agency	The Environmental Protection Agency analyzes health risks caused by toxic chemicals, emissions from vehicles, and other sources of pollution. It examines the extent to which such pollutants may cause health problems and it sets and recommends policies or regulations to minimize the risk to the public.
Department of Defense	The Department of Defense uses a risk management approach to protect its forces. For example, it has used risk management to identify threats and vulnerabilities, and determine which assets are the most critical and to make management decisions on how to make its bases and related facilities more secure.

Source: GAO.

Application of Risk Management to Homeland Security Is Widely Endorsed and Accepted

Risk management was part of the nation’s approach to assessing terrorism before the events of September 11. For example, in the 1990s, the Defense Special Weapons Agency assessed risks to evaluate force protection security requirements for mass casualty terrorist incidents at military bases. Companies under contract to federal agencies such as the Department of Energy, the National Security Agency, and the National Aeronautics and Space Administration used risk assessment models and methods to identify and prioritize security requirements. The Federal Aviation Administration and the Federal Bureau of Investigation did joint threat and vulnerability assessments on airports determined to be high risk. When we reviewed two of these efforts in the late 1990s, we found a lack of formal risk assessment requirements and made several recommendations to integrate risk-based data into decision-making processes.[3]

What September 11 changed was the intensity and magnitude of this task. The September 11 attacks were clearly a transformational event for the nation, in that they called attention to vulnerabilities throughout the nation's infrastructure, not just in aviation security. While there might always have been a concern, for example, about the consequences of an accident in a chemical factory in a highly populated area, now, these consequences had to be viewed not just from the standpoint of a potential accident, but as something a terrorist could exploit. Potential targets multiplied, and the scope of work to be done became much greater. Homeland security spending rose from about $21 billion in fiscal year 2001 to a proposed $50 billion in fiscal year 2006.

Risk management has received widespread support and interest from Congress, the President, and the Secretary of DHS as a tool that can help set priorities on how to protect the homeland. In this setting, numerous and substantial gaps in security exist, but resources for closing these gaps are limited and must compete with other national priorities. Policymakers in the legislative and executive branches have endorsed risk management as a technique that can inform decisions on setting relative priorities and on making spending decisions.

In view of the widespread support that risk management has gained, federal agencies are now required to assess risks. The Homeland Security Act of 2002 calls for a comprehensive assessment of risk related to vulnerabilities of critical infrastructure and key resources, notably (1) the risk posed by different forms of terrorist attacks, (2) the probability that different forms of an attack might succeed, and (3) the feasibility and efficacy of countermeasures to deter or prevent such attacks.[4] Two congressionally chartered commissions, the 9/11 Commission and the Gilmore Commission, support the use of data on risks to help inform the difficult decisions that must be made in allocating limited federal funds for

[3] GAO, *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, GAO/NSIAD-98-74 (Washington D.C.: Apr. 9, 1998), and GAO, *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks*, GAO/NSIAD-99-163 (Washington, D.C.: Sept. 14, 1999).

[4] 6 U.S.C. 201(d)(1), (2).

security measures. The President has issued policies directing the heads of seven major departments or agencies to assess risks. The past and present Secretaries of DHS have stated that actions of the department will be guided through the use of risk management.

Department of Homeland Security Has Broad and Challenging Responsibilities in Applying Risk Management

Congress has charged DHS with lead responsibilities in carrying out or coordinating homeland security programs and for applying risk management in carrying out this responsibility. For two main reasons, integrating a risk management approach into its business practices is a major management challenge that faces DHS.

- First, relative to many other fields such as insurance or finance, terrorism is a relatively new application for risk management. The sources of the risk are intelligent adversaries with malevolent intent with whom there is relatively little domestic experience. Unlike the insurance or banking industries, which have extensive historical data that are used to assess risks, DHS lacks such data on domestic terrorism, and this limits any detailed analysis in assessing risk. As a result, the probabilities and consequences of a terrorist act are poorly understood and difficult to predict and greater reliance on expert judgment is required. In January 2005, we identified risk management as an emerging high-risk area. At that time, we noted that DHS had not completed any risk assessments mandated by the Homeland Security Act.[5]

- Also, the size and complexity of homeland security activities add another dimension of difficulty to the task. Since its inception in March 2003, DHS has been faced with the challenge of transforming 22 agencies into one department in a way that results in an organization with effective planning, management, and operations while carrying out its critical mission of securing the homeland. Since 2003, we have designated implementing and transforming DHS as high risk, because DHS had to transform these many agencies—several with major management challenges—into one department.[6] Besides the challenge it poses at the federal level, risk management also crosses jurisdictional boundaries and involves state and local governments and private industry stakeholders, and it requires a multidisciplinary

[5] GAO, *High-Risk Series: An Update*, GAO-05-207, p.29 (Washington, D.C.: January 2005).

[6] GAO-05-207.

approach involving intelligence, law enforcement, strategic planning, and program activities that address threats and vulnerabilities.

Within DHS, we examined the progress of three DHS components—the Coast Guard, ODP, and IAIP—in administering risk management as part of their management processes. Two of these components (Coast Guard and ODP) have responsibilities related to seaport security. IAIP's responsibilities are much broader and more difficult—it is responsible for coordinating and assessing homeland risks across the federal government. Here is an overview of the three components.

- *The United States Coast Guard*. The Coast Guard is the lead federal agency for the security of the nation's ports. Its responsibilities include protecting ports, the flow of commerce, and the maritime transportation system from terrorism. As the lead in domestic maritime security, the Coast Guard has a robust presence at the national, regional, and port levels. The Coast Guard protects more than 300 ports and 95,000 miles of coastline. By providing a secure environment, the Coast Guard keeps maritime transportation open for the transit of commercial goods, as well as assets and personnel from the armed forces. In carrying out its mission, the Coast Guard has, among other activities, conducted local and national assessments of security risks at the nation's ports. The role of the Coast Guard in applying risk management to port security is discussed in more detail in chapter 2.

- *The Office for Domestic Preparedness*. Within the Office of State and Local Government Coordination and Preparedness, the Office for Domestic Preparedness is responsible for administering federal homeland security assistance programs for states and localities, including the port security grant program. Since 2002, the program has awarded over $500 million in grants to state, local, and industry stakeholders to improve security in and around their facilities or vessels. The role of ODP in applying risk management to port security grants is discussed in more detail in chapter 3.

- *Information Analysis and Infrastructure Protection Directorate*. The Information Analysis and Infrastructure Protection Directorate is responsible for, among other things, identifying and assessing current and future threats to the homeland, mapping those threats against known vulnerabilities, recommending protective measures, issuing warnings, and offering advice on preventive and protective action. IAIP is responsible for cataloging key critical infrastructure, then analyzing various characteristics to prioritize this infrastructure for the entire nation. These priorities are then to be used to direct protective measures for port security as well as across all other kinds of infrastructure. The role of IAIP in applying risk management to ports and other infrastructure is discussed in more detail in chapter 4.

Seaports Are an Important Focus in the Homeland Security Response

Seaport security receives substantial focus in this report because seaports have been widely regarded as vulnerable to attack. One reason is that the nation's seaports and inland waterways play a vital role in the nation's economy and national security. From an economic perspective, ports are critical links in the commercial trade and transportation systems, with more than 95 percent of the nation's non-North American foreign trade, including 100 percent of foreign oil, entering the country through seaports. The range of commodities involved includes not only a wide variety of consumer and agricultural products, but also cargo considered dangerous such as liquefied petroleum gas. A significant portion of this waterborne trade comes via cargo containers that are expected to move in and out of ports quickly, in keeping with industry expectations of just-in-time delivery. Port facilities are also used to ship military cargo abroad, and the Departments of Defense and Transportation have designated about 17 ports as "strategic" to support wartime mobilization, deployment, and resupply. Finally, not only are ports key hubs in our transportation system, they also function as centers of industrial, commercial, and financial activity. As such, they are home to many assets that are deemed to be among the nation's most critical infrastructure, which is to be protected under the USA PATRIOT Act of 2001 and the Homeland Security Act of 2002.

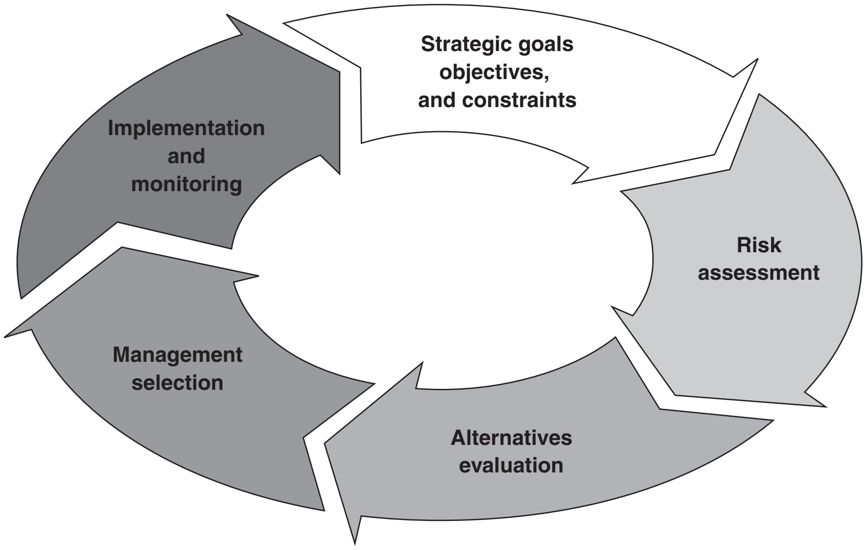
A second reason that seaports are potentially vulnerable is the wide range of targets and attack possibilities they encompass. Facilities such as container terminals, where containers are transferred between ships and railroad cars or trucks, must be able to screen vehicles entering the facility and routinely check cargo. Chemical factories and other installations where hazardous materials are present must be able to control access to areas containing dangerous goods or hazardous substances. Vessels, ranging from oil tankers and freighters to tugboats and passenger ferries, must be able to restrict access to onboard areas, such as the bridge or other control stations critical to the vessels' operation. Possible terrorist scenarios range from the use of improvised explosive devices to attack ferries to the use of recreational boats to ram key infrastructure in and around ports.

A Framework for Risk Management

While there is a consensus that risk management should be applied to homeland security programs, doing so is a complex task that has few precedents and little specific guidance. The Homeland Security Act and presidential directives have called for the use of risk management. However, they did not define how risk management was to be accomplished. Given that there are no established universally agreed upon set of requirements or processes for risk management of homeland security, we developed a framework that can be broadly applied to a range of settings, such as analyzing security in the maritime sector and other environments. We did so by gathering, reviewing, and analyzing an extensive amount of public and private sector work; interviewing experts from private consulting companies in the areas of risk management and risk computer-modeling; interviewing experts on terrorism; and utilizing our own past work in this area. We also solicited comments and feedback from academic experts in risk management. As part of our work, we briefed officials of the three DHS components about the various phases of the framework, and the officials generally agreed with its structure and intent. The application of risk management to homeland security is relatively new, and the framework will likely evolve as processes mature and lessons are learned.

The framework we developed is a conceptual synthesis of risk management approaches that we use as criteria to assess the adequacy of DHS's risk management systems (see fig. 2). For further information on the framework and how we developed it, see appendix I.

Figure 2: A Framework for Risk Management



Source: GAO.

This framework may be applied governmentwide and at various organizational levels, from departmental down to individual programs. The figure illustrates the cyclical nature of this approach, and while the phases are generally linear, changes can be made at any step in the process as new information becomes available. The five major phases of risk management are detailed below.

Strategic Goals, Objectives, and Constraints

According to the framework, management decisions are to be made in the context of the organization's strategic plan, with clearly articulated goals and objectives that flow from the plan. Performance measures that are clear, concise, and measurable are linked to the broader goals and can be used to measure progress toward these goals. An organization's program and risk planning documents address risk-related issues that are central to its mission.[7] However, various constraints can take many forms and have an impact on risk related strategies. For example, some constraints may be imposed by statute, organizational policy, or budget restrictions. Managers at different levels within an agency or organization may encounter various constraints that differ with the scale of the operation.

[7] For reasons of security, this identification may not be public knowledge.

Risk Assessment

Risk assessment helps decision makers identify and evaluate potential risks facing key assets or missions so that countermeasures can be designed and implemented to prevent or mitigate the effects of the risks.[8] In our framework, risk assessment is a function of threat, vulnerability, and consequence. The product of these elements is used to develop scenarios and help inform actions that are best suited to prevent an attack or mitigate vulnerabilities to a terrorist attack, in conjunction with the risk-based evaluation of alternatives undertaken while considering cost and other factors.

- *Threat* is the probability that a specific type of attack will be initiated against a particular target/class of targets. It may include any indication, circumstance, or event with the potential to cause the loss of or damage to an asset. It is based on an understanding of an adversary's intention, motivation, history of attacks, and capability to do damage. Analysis of threat-related data is a critical part of risk assessment. Information for characterizing threat can be gained from a variety of sources, such as the intelligence and law enforcement community, as well as from past activities of various terrorist groups. Understanding an underlying pattern of attacks on target types is useful in predicting future terrorist events and planning mitigation strategies. However, the unexpected threats not contained in the historical record of terrorist groups also need to be considered. Ultimately, one purpose of assessing threats is to assign relative probabilities to various types of attacks.

- The *vulnerability* of an asset is the probability that a particular attempted attack will succeed against a particular target or class of targets. It is usually measured against some set of standards, such as availability/predictability, accessibility, countermeasures in place, and target hardness (the material construction characteristics of the asset). Each of these four elements can be evaluated based on a numerical assignment corresponding to the conditional probability of a successful attack. The probability that a particular vulnerability could be successfully exploited is, in part, a function of the effectiveness of the antiterrorism countermeasures.

- The *consequence* of a terrorist attack is characterized as the expected worst case or worse reasonable adverse impact of a successful attack.

[8] A countermeasure is any action taken or physical equipment used principally to reduce or eliminate one or more vulnerabilities.

> The consequence to a particular asset can be evaluated when threat and vulnerability are considered together. The outcome of a terrorist attack may include many forms, such as the loss of human lives, economic costs, and adverse impact on national security.

Another closely related element taken into consideration is criticality (that is, the relative importance) of the asset involved. Criticality involves the prioritization of assets based on factors such as the potential for loss of life and the economic implications for the livelihood, resources, or wealth of the area, region, or country if the asset were to be lost. Layers of effective security countermeasures increase the likelihood that a terrorist attack will be unsuccessful as risk is reduced.

Alternatives Evaluation

Risks can be reduced through various antiterrorism countermeasures or countermeasure systems designed to prevent an attack or mitigate the impact of an attack. Two concepts here are key to evaluating countermeasure alternatives. The first is that countermeasures should be evaluated against specific risk assessments to determine the extent to which risks can be reduced by the countermeasure being considered. The second concept is the role of costs to both public and private sources, as costs are a critical element in the application of countermeasures. In our framework, cost-benefit analysis is critical in assessing alternatives, because it links the benefits derived from risk-reducing alternatives to the costs associated with implementing and maintaining them.

Management Selection

Management selection in our framework is informed by the outputs in the preceding phases. Having assessed risks and evaluated countermeasure options, management selects the blend of intervention strategies and activities across the entire spectrum of goals, objectives, and components of risk that achieves the greatest expected risk reduction in relation to cost for both the short and the long term among the various proposed alternatives. However, the technical analysis of alternatives is not likely to resolve or fully capture the numerous elements of concern to management. Decision makers may employ various risk-reducing strategies. However, preferences and value judgments will influence decisions about which strategies to employ. For example, corporate culture may influence decision makers to concentrate countermeasures on a relatively few critical assets, while others may value distributional impacts, that is, some organizations may be more willing than others to distribute resources over a wider array of assets. Management selection is an important task, and decisions are made with the information that is available. Our guidelines for effective internal controls dictate that once decisions are reached, they, along with the rationales for them, should be documented in order to inform future actions.

Implementation and Monitoring

This phase in the framework involves the implementation of the selected countermeasures. Following implementation, monitoring is essential in order to help ensure that the entire risk management process remains current and relevant, and reflects changes in the effectiveness of the alternative actions and the risk environment in which it operates. It is crucial to exploit any and all information sources, exercises, gaming, modeling and simulation, analysis of real world events, and sharing of information in a data sparse environment. Measurable objectives show the degree to which activities, timelines, support functions, service delivery, and spending are consistent with goals and implemented in accordance with the planning process. Program evaluation is an important tool for assessing the efficiency and effectiveness of the program. In addition to simply monitoring the implementation of the system and making adjustments, the entire risk management planning process should be periodically revisited. Since technology and information change at a rapid pace, countermeasures in place today may be outdated tomorrow and may become more susceptible to being breached. In addition, consultation with external subject area experts can provide a current perspective and an independent review in the formulation and evaluation of the program.

Objectives, Scope, and Methodology

Our overall aim was to provide a perspective on how three DHS components have applied risk management as it relates to homeland security in general, or to port security in particular. More specifically, this report addresses the following objectives:

- What progress has the Coast Guard made in applying risk management to its port security mission, and what challenges does it face in moving further?
- What progress has ODP made in applying risk management to its administration of the port security grant program, and what challenges does it face in moving further?
- What progress has IAIP made in applying risk management to comparing and prioritizing critical infrastructure with one another and what challenges does it face in moving further?

- Are there key observations that can be drawn from all three of these efforts with regard to how far the three components have come in risk management as it applies to terrorism?

To determine what progress the Coast Guard has made in applying risk management to its port security mission and the challenges that it faces, we met with Coast Guard officials responsible for port security risk assessment efforts to discuss the progress they have made and the challenges that remain. We discussed risk management efforts and challenges with Coast Guard officials at four ports—Baltimore, Maryland; Charleston, South Carolina; Houston, Texas; and Seattle, Washington—who were responsible for risk management activities. We judgmentally selected these ports because of their geographic distribution, and the results from our interviews cannot be generalized to ports nationwide. In addition, we reviewed documents of the Port Security Assessment Program, the Port Security Risk Assessment Tool, Area Maritime Security Plans, the National Risk Assessment Tool, the National Maritime Security Profile, and the National Maritime Strategic Risk Assessment. We also reviewed key legislation such as the Maritime Transportation Security Act of 2002 and prior GAO reports on maritime security. Finally, we reviewed threat assessments produced by the National Maritime Intelligence Center and the Transportation Security Agency to gain a more complete understanding of the challenges.

To determine what progress ODP has made in applying risk management to its administration of the port security grant program and the challenges that it faces, we compared fiscal year 2004 and fiscal year 2005 ODP port security grant program procedures. In order to understand the grant process and the risks related to individual ports, we reviewed the risk assessment tools used by ODP officials, including the Coast Guard's Port Security Risk Assessment Tool.[9] We reviewed and summarized a database listing fiscal year 2004 grant applications and awards to determine the extent to which criteria for awards coincided with the receipt of grant awards. We reviewed the Inspector General's (IG) January 2005 report of the port security grant program and discussed the recommendations contained in the report with ODP officials. We examined procedural changes made by ODP, in response to the IG recommendations and other factors, to the 2005 grant application process. We did not review the fiscal

[9] The Coast Guard Port Security Risk Assessment Tool is designed to be used by the Captains of the Ports when making risk-based analyses of assets in their area of responsibility.

year 2005 award decisions because we had completed our fieldwork before award decisions were announced, in September 2005. We met with Coast Guard, Maritime Administration, ODP, and IAIP officials involved in the port security grant program process. We also reviewed pertinent legislation, such as appropriations for the grant program for successive fiscal years.

To determine what progress IAIP has made in applying risk management to comparing and prioritizing critical infrastructure, and what challenges it faces in moving ahead, we reviewed key legislative and executive documents, such as the Interim National Infrastructure Protection Plan, the Homeland Security Act of 2002, Homeland Security Presidential Directives 7 and 8, national strategies, and DHS's strategic plan. We met with IAIP officials responsible for identifying and prioritizing threats, vulnerabilities, and consequences across different types of critical infrastructure to determine the obstacles they face in making such evaluations and the challenges they face in making progress in this area. We reviewed documents, such as the Risk Analysis and Management for Critical Asset Protection and the Buffer Zone Protection Program. We interviewed Office of Management and Budget (OMB) officials responsible for oversight of issues involving infrastructure protection to obtain their views on risk management practices across the federal government.

To determine whether there are key observations that can be drawn from the three components we reviewed, we analyzed and synthesized the findings we developed to identify challenges that remain in applying risk management to homeland security. We compared the three components' progress in applying risk management principles to their respective tasks, identified common experiences in applying risk management, and drew conclusions about issues that may need addressing. We reviewed numerous documents, including pertinent statutes and presidential directives, GAO reports on high-risk programs in the federal government, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and testimony by the Secretary of DHS.

We performed our work in accordance with generally accepted government auditing standards between May 2004 and November 2005.

Chapter 2: The Coast Guard Has Made Progress in Using Risk Management, but Challenges Remain

The Coast Guard has established a foundation for applying risk management to port security; its next challenges are to refine and strengthen its approach. The Coast Guard has made progress in all five phases of risk management (see table 2). For the first phase—goals and objectives—the Coast Guard has established broad strategic goals for port security, and its next challenge is to translate these goals into specific, measurable objectives that can be used to assess performance. The Coast Guard has actions under way to address this challenge—a key step in determining the extent to which its actions actually reduce risk. The Coast Guard has made the most progress in the second phase—conducting risk assessments. Six separate but related assessment efforts, covering both individual ports and the nation as a whole, have given the Coast Guard a clearer sense of the vulnerabilities that exist. However, current assessments are limited in terms of their methodology, and they do not allow the Coast Guard to compare and prioritize relative risks across ports—limitations that the Coast Guard recognizes and is taking steps to address. Enhancing these first two risk management phases is key to making further progress on the next two phases—evaluating risk mitigation alternatives and selecting a particular alternative for action. Without measurable objectives and more complete methodologies, the risk management process may not be able to target the most significant security concerns or determine the most cost-effective approach to take in providing reasonable protection. Additionally, weaving data produced from the risk management process into the annual cycle of program review remains a challenge. Finally, with regard to the fifth phase—implementation and monitoring—the Coast Guard has demonstrated the ability to evaluate its efforts and make improvements. However, more extensive and more formal feedback mechanisms would help ensure that Coast Guard headquarters managers can inform field staff about actions taken as a result of the comments received about the risk management process. The Coast Guard has actions under way to improve feedback loops.

Table 2: Summary of Progress Made and Challenges That Remain in the Coast Guard's Risk Management Approach

Risk management phase	Examples of progress made	Examples of remaining challenges
Strategic goals, objectives, and constraints	High-level strategic goals have been set for port security nationwide and for port locations across the country.	High-level goals have not been translated into measurable objectives. The Coast Guard recognizes the importance of developing measurable objectives and is working to do so.
Risk assessment	Several types of risk assessments have been conducted at both the port and the national level. They have given the Coast Guard the ability to compare and prioritize infrastructure within a port.	Data on threats, vulnerabilities, and consequences have limitations. Methods have not been developed to allow the Coast Guard to compare and prioritize risks across ports. Coast Guard officials agreed they have challenges and are taking action to address them.
Alternatives evaluation	Using local risk assessments, the Coast Guard has developed alternative approaches to prevent attacks and reduce vulnerabilities.	At the national level, the Coast Guard's methodology for evaluating alternatives is limited. National risk assessments generally lack cost and benefit data on alternative ways to mitigate port security risks. The Coast Guard is taking steps to address this challenge by examining benefits (reductions in risk) and the estimated costs in doing so.
Management selection	Coast Guard officials have been able to use expert knowledge or data from risk assessments to select specific alternatives, such as establishing security zones around key infrastructure, improving security around ferries and cruise ships, and coordinating security improvements (such as fences, gates, and cameras) around key infrastructure.	Methodological limits in risk assessments and alternatives evaluation hinder the quality of data that informs management decisions. Informing the annual cycle of program review with data from risk management processes has been limited. The Coast Guard recognizes these challenges and has actions under way to address them.
Implementation and monitoring	The Coast Guard has implemented improvements to some of its risk assessment tools to make them stronger and has invited feedback from staff on how processes are working.	Existing feedback mechanisms are limited to largely informal processes, reducing communication between headquarters and field staff about actions taken as a result of the comments or feedback provided. The Coast Guard plans to include formal feedback loops in one of its risk assessment tools by the end of 2005.

Source: GAO analysis of the Coast Guard's risk management efforts.

Coast Guard Homeland Security Activities Revolve Heavily around the Maritime Domain

The Coast Guard is the lead federal agency responsible for protecting domestic ports. In this role, the Coast Guard must identify, evaluate, and mitigate many kinds of security challenges. Ports are often sprawling enterprises that contain key infrastructure besides docks, piers, ships, barges, and warehouses. Many ports are also home to power plants, chemical factories, bridges and tunnels, and a variety of other assets of critical importance to the nation's economy and its defense.

Coast Guard expenditures and activities for port security have risen dramatically since the terrorist attacks of September 11. The Coast Guard estimates that its budget for port security has jumped from about $250 million in fiscal year 2001 to about $1.5 billion in fiscal year 2005. Since the terrorist attacks, the Coast Guard has carried out a myriad of port security activities, including increasing its intelligence capabilities, carrying out more harbor patrols and vessel escorts, establishing security zones, and working more extensively with federal, state, local, and industry stakeholders on port security matters as required by the Maritime Transportation Security Act of 2002 (MTSA).

While much of the Coast Guard's homeland security efforts center specifically on ports, these activities are part of the agency's broader mission of Ports, Waterways, and Coastal Security (PWCS). This mission involves protecting the maritime domain and marine transportation system; preventing terrorist attacks, and responding to and recovering from attacks that do occur.[1] As part of the PWCS mission, the Coast Guard aims to develop greater "maritime domain awareness"—that is, improving port stakeholders' understanding about anything associated with the global maritime environment that could adversely affect the security, safety, economy, or environment of the United States. Maritime domain awareness seeks to identify threats as soon as possible and far enough away from domestic ports to eliminate or mitigate the threat. Several Coast Guard efforts are under way to help address both port security and marine domain awareness. In particular:

[1] U.S. Coast Guard, *Maritime Sentinel: Coast Guard Strategic Plan for Ports, Waterways, and Coastal Security* (Washington D.C.: September 2005). According to Homeland Security Presidential Directive 13 on Maritime Security Policy (Dec. 21, 2004), maritime domain means all areas and things of, on, under relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime related activities, infrastructure, people, cargo, and vessels and other conveyances.

- The Coast Guard is planning to expand its sector command centers, where officials can receive data 24 hours a day on maritime activities. Currently, the Coast Guard plans to develop sector command centers at 35 ports.[2]

- The Coast Guard is involved in a major recapitalization effort—called the Integrated Deepwater System—to replace and modernize the agency's aging fleet of aircraft and vessels, including improved and integrated command, control, communications and computers, intelligence, and surveillance and reconnaissance capabilities. Since the terrorist attacks of September 11, the Coast Guard has revised its plans, and the Deepwater program now includes improving maritime domain awareness and maritime security capabilities as part of its mission. This program is scheduled to take 20 years and cost between $19 billion and $24 billion.

Federal statutes and presidential directives call for the Coast Guard to use risk management in its homeland security efforts. MTSA, for example, calls for the Coast Guard and other port security stakeholders to carry out a variety of risk-based tasks, including assessing risks and developing security plans for ports, facilities, and vessels.[3] The Coast Guard's progress across the various risk management phases is thus a key part of its homeland security mission. The remainder of this chapter discusses the Coast Guard's progress and challenges on each of the phases in GAO's framework.

[2] According to the Coast Guard, there are 30 sectors with command centers already in place.

[3] See 46 U.S.C. § 70103(b), (c); 33 C.F.R. §§ 103.400, 103.500, 104.300, 104.400, 105.300, and 105.400.

Goal-Setting: High-Level Goals Are in Place, with Efforts Under Way to Set Measurable Objectives

The Coast Guard has been able to make some progress in the first phase of the risk management framework, in that it has established high-level strategic goals for its PWCS mission. The Coast Guard set its national strategic goals for port security in December 2002.[4] In order of priority, the goals were as follows:

- preventing terrorist attacks within, and terrorist exploitation of, the maritime domain;
- reducing America's vulnerability to terrorism in the maritime domain;
- protecting population centers, critical infrastructure, maritime borders, ports, coastal approaches, and the boundaries and seams between them;
- protecting the U.S. marine transportation system while preserving the freedom of the maritime domain for legitimate pursuits; and
- minimizing the damage and expediting the recovery from attacks that may occur within the maritime domain as either the lead federal agency or a supporting agency.

Working with federal, state, local, and industry stakeholders involved in port security, the Coast Guard has also developed security plans for port areas across the country. These plans reflect the characteristics and needs of the individual ports, and in general, they aim to deter a terrorist incident and improve communication among port stakeholders. These plans are specific to each port location and are aligned with higher-level port security goals.

While the Coast Guard has set broad goals for its port security mission, it still faces challenges in developing objectives into more specific and measurable results that measure progress toward these goals. So far, the Coast Guard has expressed its port security objectives in terms of activity levels, such as conducting patrols, escorting vessels, and inspecting cargo. While such activities may have contributed to improved security in and around the nation's ports, using them as measures may not systematically target areas of higher risk and may not result in the most effective use of resources, because these measures are not pointed toward outcomes. They describe what levels of activity, or outputs, the Coast Guard is providing, but they do not provide an indication of what these activities are accomplishing. Doing so requires measures that are clearly tied to

[4] U.S. Coast Guard, *Maritime Strategy for Homeland Security* (Washington, D.C.: December 2002).

results. Such measures would indicate the extent of progress made and help identify the security gaps that still remain.[5]

Developing measurable objectives is a complex and difficult task, but Coast Guard officials recognize that doing so is a necessary next step and plan to have such objectives developed in fiscal year 2006. In September 2005, the Coast Guard stated that it plans to develop a measure of its performance that will be based on an assessment of threat, vulnerability, and consequence. The Coast Guard plans to develop objectives for reducing overall risk. As part of this process, the Coast Guard plans to assess the impact of its activities in reducing threats, vulnerabilities, and consequences.

Risk Assessments: Progress Has Been Substantial, but Challenges Remain for Addressing Limitations in Assessment Data and Methodology

The Coast Guard's risk management activities have centered primarily on this phase of the risk management process, with assessments being conducted at both port and national levels. Further progress on the quality of these assessments is challenged by several types of limitations in the data and the methodology being used.

Several Sets of Assessments Have Been Completed at the Port and National Levels

Following the terrorist attacks of September 11, and consistent with MTSA's directives, the Coast Guard has greatly expanded the scope of its risk assessment activities. Before the attacks, these assessments centered on matters such as ecological damage and general marine safety. In 1999, for example, the Coast Guard adopted a risk management approach for its

[5] Any goals that the Coast Guard establishes will need to be aligned with two other national efforts to protect critical infrastructure. First, Homeland Security Presidential Directive-7 establishes a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources, including assets and resources in and around ports. Second, Homeland Security Presidential Directive-13 establishes policy and guidelines for implementing actions that enhance maritime security. The policy includes (1) preventing terrorist attacks and reducing vulnerabilities to attacks in the maritime domain; (2) enhancing security of ports, critical infrastructure, and coastal approaches; (3) enhancing international relationships; and (4) ensuring coordinated implementation of authorities and responsibilities among federal departments and agencies.

marine safety and environmental mission area. Assessments of key infrastructure in and around ports came largely after the attacks. Three such assessments have been done at the port level (see table 3).[6] These assessments included data on threats, vulnerabilities, and consequences—the three types of information used in evaluating risk:

- *Threats*. The assessments gathered information on plausible threat scenarios, such as using weapons of mass destruction, ramming a vessel or facility, or detonating devices underwater. In general, local Coast Guard personnel or other federal and nonfederal stakeholders decided what threat scenarios to include in the assessment based on their knowledge of the port.

- *Vulnerabilities*. The assessments evaluated threat scenarios against potential targets, such as passenger vessels, bridges, or terminals, to assess the degree to which these potential targets were vulnerable to attack.

- *Consequences*. Finally, the three assessments addressed the potential outcomes of successfully carrying out a threat against a potential target. These consequences included such matters as loss of life, damage to the environment, damage to property, and economic disruption.

[6] We previously reported on two of these efforts—the area maritime security assessments and the Port Security Assessment Program. See GAO, *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security*, GAO-04-838 (Washington D.C.: June 30, 2004), and *Maritime Security: Better Planning Needed to Help Ensure an Effective Port Security Assessment Program*, GAO-04-1062 (Washington D.C.: Sept. 30, 2004).

Table 3: Port-Level Assessments Conducted by the Coast Guard

Port-level risk assessment	Description
Port Security Risk Assessment Tool (PS-RAT)	Implemented in November 2001, PS-RAT is a computer-based tool for determining the risk associated with specific attack scenarios against key infrastructure or vessels in local ports. It was used to compare and prioritize risks among critical infrastructures at a port. In November 2002, the Coast Guard improved the tool to address inconsistencies in data among ports, and it included additional factors for mitigation, such as recoverability from an attack.
Port Security Assessment Program	Begun in August 2002 and completed in March 2005, this program produced a vulnerability assessment of 55 of the nation's most strategic commercial and military ports. To identify which ports were of the most strategic importance, the Coast Guard considered such factors as cargo volume, ferry and cruise ship traffic, population density around the port, and presence of critical infrastructure.
Area Maritime Security Plans	Required under the Maritime Transportation Security Act of 2002, these plans describe a communication and coordination framework for port stakeholders and law enforcement officials to follow in addressing security vulnerabilities and responding to incidents. The Coast Guard has completed plans for all 43 designated port areas.

Source: GAO analysis of the Coast Guard's port-level assessments.

These assessments have resulted in considerable progress in understanding and prioritizing risks within a port. In particular, the Port Security Risk Assessment Tool (PS-RAT), a computer program that includes possible threat scenarios, allows the Coast Guard to assess risks and develop relative rankings for infrastructure at each port location. At one port, PS-RAT was used to compare and inform priorities on over 1,000 critical items of infrastructure.

Three other efforts have focused on assessments at the national level (see table 4).[7] These efforts have relied in part on data and information generated from the local assessments described above, but they have also incorporated additional information. For example, the National Maritime Security Profile integrated available information from the intelligence community—a step that had not been carried out in any of the local risk assessments. Another assessment, the National Maritime Strategic Risk Assessment, sought to develop risk profiles for each of the Coast Guard's strategic goals; it examined specific mission areas, including port security, search and rescue, and law enforcement, and it sought input from field commanders on ways to mitigate key risks. According to Coast Guard

[7] In addition to these efforts, the Coast Guard was involved in an interagency effort called the National Maritime Transportation Security Plan. This effort included the results of the National Maritime Security Profile. According to the Coast Guard, the results of the plan will contribute to the Coast Guard's outcome measures for its PWCS mission.

staff, this was the first attempt at a large-scale strategic risk assessment that sought to assess the status of the maritime domain.

Table 4: National-Level Assessments Conducted by the Coast Guard

National-level assessments	Description
National Risk Assessment Tool	Implemented in February 2002, this tool provided a foundation for strategically evaluating the risks in the maritime domain. It incorporated 50 types of infrastructure and 12 possible attack scenarios and included information on threat, vulnerability, and consequences. Information from the local tool (PS-RAT) was used in developing the results.
National Maritime Security Profile	Developed in 2003-2004, this profile assessed critical infrastructure, possible threats, vulnerabilities, and consequences. It used PS-RAT and the national risk assessment tool, among other methods, to develop the profile, and it gathered input from the intelligence community to improve data on threats for its PWCS mission.
National Maritime Strategic Risk Assessment	Launched in August 2004, this is an effort to communicate risks in each of the Coast Guard's missions. As part of this risk assessment, the Coast Guard used information from the National Maritime Security Profile. Among other things, this effort identified possible intervention strategies for addressing risk areas.

Source: GAO analysis of the Coast Guard's national-level assessments.

While the port-level assessments focus on specific assets and infrastructure at each location, national assessments have focused more generally on understanding the risk posed to various classes of assets (such as container ships, barges, power plants, or bridges and tunnels) by various types of attacks (such as using explosives, taking control of an asset, or using weapons of mass destruction). These national assessments address, for example, whether the maritime domain is at greater risk from a takeover of a power plant or from a weapon of mass destruction planted on a container ship. The national assessments do not compare risks faced by specific assets at one port with risks faced by specific assets at another port.

Key Challenges Involve Improving Data and Methodology

The progress in conducting risk assessments is tempered by a number of challenges that remain in making these assessments more robust tools for informing the risk management process. These challenges are numerous and complicated, and this chapter illustrates some of the important issues the Coast Guard faces in making its risk assessments more useful. The challenges discussed here involve (1) improving the threat, vulnerability, and consequence data on which the assessments are based and (2) addressing methodological limitations that affect the reliability, completeness, and applicability of the risk assessments themselves.

Limitations of Data on Threats, Vulnerabilities, and Consequences

Our review of the Coast Guard's processes and our discussions with Coast Guard personnel surfaced a number of data-related problems that limit the reliability and completeness of the risk assessments (see table 5). For example, the tools require information not only about the types of threats a facility may face, but also about the probability of such threats occurring. The threat data received by the Coast Guard from the intelligence community do not allow the Coast Guard to model these probabilities, thus limiting the value of the output. The problems we identified have implications for the ability to effectively compare risks faced by the various types of port-related infrastructure.

Table 5: Examples of Data-Related Challenges in Coast Guard Risk Assessments

Data type	Summary of challenge
Threats	The information received from intelligence sources is generally useful, but it lacks the detail that allows the Coast Guard to model the relative probability of various threat scenarios. For example, the Coast Guard cannot assign a relative probability to various threat scenarios, affecting the ability to characterize threats without either understating or overstating them. In practice, the calculation of threat was essentially held constant for Coast Guard-wide analysis of PS-RAT data.
Vulnerabilities	The Coast Guard's tools for assessing risk currently do not take into account (1) reductions in vulnerability that stem from the Coast Guard's actions (such as security patrols or other monitoring) or (2) the effect that multiple strategies (such as fencing and guards) may have on reducing vulnerabilities. As a result, the tools may overstate the degree of vulnerability that exists.
Consequences	The Coast Guard's tools measure the direct effects of a terrorist attack, such as loss of lives and property damage, but they do not consider the secondary effects, such as loss of jobs that may occur. This limitation likely understates the overall consequences resulting from an attack.

Source: GAO analysis of the Coast Guard's risk assessment efforts.

These challenges are complex and technical, and the following examples illustrate the kinds of limitations they pose:

- *Limitations in threat-related data.* The intelligence information the Coast Guard normally receives about threats is not specific enough for all of the threat scenarios in the National Maritime Security Profile or the PS-RAT.[8] For example, the type of threat data that Coast Guard personnel could use to model threats includes data on the presence of terrorist cells nationally and internationally, the capability and intent of terrorist groups as they relate to specific types of attack in and around ports, and the specific target groups. Increasing the quality of this

[8] The threat scenarios examined by the Coast Guard are contained in documents that are considered sensitive and for official use only. Accordingly, we do not provide detailed examples of various threat scenarios evaluated by the Coast Guard.

information would improve the quality of the output. For example, when the Coast Guard received and integrated higher-quality information about some threats from its Intelligence Coordination Center, it modified data for 80 of about 300 threat scenarios in its National Maritime Security Profile.

- *Limitations in vulnerability-related data.* The Coast Guard's risk assessment tools were designed to evaluate existing security in and around a building or vessel, but according to Coast Guard officials, the baseline established by the tools excludes areawide actions the Coast Guard has taken to reduce vulnerabilities in and around ports, such as conducting more patrols, creating operational centers, or establishing security zones in and around key ports. The baseline also excludes actions taken by local port stakeholders, such as increasing the number of harbor patrols conducted by local law enforcement. The Coast Guard designed its tools this way because the primary purpose of the tools was to provide a port-level risk ranking of assets. Using this information, the Coast Guard could then use tools, such as the PS-RAT, to measure the benefit and value of any interventions for a specific vessel, facility, or asset type that it initiates against the original baseline. Coast Guard officials recognize that another tool would be useful in determining the overall vulnerabilities that exist after all Coast Guard actions have been taken.

- *Limitations in consequences-related data.* The Coast Guard's assessment of consequences is limited to direct effects of a terrorist attack, such as loss of lives and property damage; it does not consider important secondary effects, such as follow-on effects to the economy, including loss of jobs or increased energy costs that may occur months after an attack. This limitation likely understates the overall consequences that result from an attack and may distort relative risks associated with various threat scenarios. Coast Guard officials note that estimating secondary effects is important but difficult since there is a lack of accepted methods for doing so. A second limitation is that there is no commonly agreed upon value for a consequence such as death or injury, or the symbolic effect of destroying a national symbol such as the Statue of Liberty. For example, the Coast Guard's model places a dollar value of $1 million (in 2005 dollars) on the loss of a life. Other components, such as the Environmental Protection Agency, use a monetary value of $6.1 million (in 1999 dollars). The value chosen can affect the priorities that emerge from using the risk assessment tools.

We discussed these data-related limitations with Coast Guard officials, who generally agreed with our observations. The Coast Guard has since planned or started several actions designed to address some of these limitations. Coast Guard officials said they plan to improve PS-RAT based in part on the limitations discussed above.[9] For example, they made changes in procedures for obtaining information from the Intelligence Coordination Center and have focused on improving the quality of information received from the intelligence community.[10] In addition, the Coast Guard plans to improve vulnerability and consequence data. For example, the Coast Guard plans to assign weights to different levels of consequences. Coast Guard officials said they hope to accomplish these changes by the end of 2005.

Methodological Limitations

Two key methodological limitations affect the use of risk assessment data as a tool for informing decision makers on relative risks across port locations. The first limitation relates directly to the ability to compare and prioritize one port with another, while the second limitation relates to the process used to rank and prioritize individual threats.

- *Risks cannot be compared between ports.* PS-RAT results were not designed to compare the risks at one port with risks at another.[11] While PS-RAT allows the Coast Guard to compare and prioritize key infrastructure within a port, it does not produce a risk ranking that permits the Coast Guard to compare and prioritize infrastructure across ports. Interport comparisons, while theoretically possible, are difficult to actualize in practice. In general terms, the difficulties stem largely from the fact that, for each port, multiple scenarios must be considered; the scenarios that are deemed most relevant to each port,

[9] Coast Guard officials said that in addition to making improvements in threat, vulnerability, and consequence data, they plan to align some of their efforts more closely with Department of Homeland Security risk assessment databases and to conduct sensitivity analyses of various mitigation strategies.

[10] IAIP officials said that the Coast Guard's efforts are a pilot project, and that if sufficiently mature, the effort will be more broadly implemented by the intelligence community.

[11] Similarly, area maritime security plans are not comparable with one another, in part because PS-RAT results underpin the plans. In addition to the limitations we describe above, the scores for each port are relative to that port and scores from one port cannot be compared with the scores from another port because, in some cases, local Coast Guard staff developed scores for asset types, such as bridges or warehouses, and at other port locations, the local staff assigned scores for individual types of assets. The Port Security Risk Assessment Program conducted studies at 55 ports at a cost of about $35 million and these studies are also not comparable with one another.

however, will differ from port to port. For example, ports that support passenger ferries and container cargo may be exposed to different risks than ports that primarily support bulk cargo. Comparisons are further limited because Coast Guard personnel at different ports use different methods to input data into PS-RAT. For example, Coast Guard officials at some field offices have summarized information on a type of asset, such as all bridges at a port location, while officials at other locations have developed data on each bridge in the area of responsibility. We discussed this limitation with the Coast Guard officials, and during the course of our review, the Coast Guard initiated work on a Maritime Security Risk Assessment Model (MSRAM)—a model that should permit the Coast Guard to compare the relative risks of high-value assets at one port with assets at a different port. The model is to include an analysis of various threat scenarios, vulnerabilities, and consequences. Overall, the MSRAM is to score and characterize risk associated with individual assets, including the estimated likelihood of an attack, the vulnerability of the asset should an attack occur, and the impacts of a successful attack. The Coast Guard has also requested data from the Intelligence Coordination Center on intent and capability that could improve the estimate of relative likelihood of various threat scenarios. Coast Guard officials said they plan to implement the MSRAM by the end of 2005.

- *Risks viewed as less probable could surprise the Coast Guard.* The Coast Guard evaluates hundreds of threat scenarios that are deemed plausible—focusing attention, ultimately, on those threats that, together with identified vulnerabilities and consequences, pose the greatest overall risk. For example, in the National Maritime Security Profile, the Coast Guard classifies the risk of various threat scenarios as very high, high, medium, low, and very low, and it centers attention on scenarios that it estimates are very high or high risk. The Coast Guard's approach, although a useful starting point, may not be as reliable as the process would appear to suggest given the data limitations we describe above. How agencies like the Coast Guard deal with scenarios that receive low rankings is important in addressing the possibility of strategic surprise—an attack scenario that may not be identified or given high priority in the initial risk assessment process. Without sensitivity analysis or formal feedback loops to reassess all scenarios and therefore provide greater assurance that the rankings are as reliable as possible, the risk of being unprepared for strategic surprise may increase.[12] The Coast Guard addresses this issue by making appropriate adjustments in priorities when tactical and strategic information call for such changes. We discussed this issue further with agency officials, and partly on the basis of these discussions, the Coast Guard is taking additional steps to address this issue. It is doing so by (1) increasing coordination among risk stakeholders at all levels to improve checks throughout the risk management cycle, (2) making refinements to threat data by requesting the Intelligence Coordination Center to provide estimates of capability and intent of terrorist groups, (3) including time horizons for various scenarios, and (4) leveraging independent assessments conducted by different subject matter experts as a way of checking its risk assessment work.

Evaluation of Alternatives: Ability to Evaluate Alternatives Is Greatest at the Local Level

Just as the Coast Guard's ability to assess risk is stronger at the individual port level than across ports, its ability to evaluate various alternatives for addressing these risks is greater at the port level as well. PS-RAT was specifically developed to help local Captains of the Port concentrate and prioritize their resources and evaluate alternative methods of risk reduction. Data from PS-RAT help identify vulnerabilities within a port and can be used in improving security measures related to the area maritime security plans. PS-RAT is not designed to work, however, above the port level. At the national level, the Coast Guard has conducted qualitative evaluations of the potential benefits of various alternatives for reducing risk levels, such as improved information sharing through the use of interagency operational centers, waterborne patrols, and escorting ships. In addition, it is assessing the potential reduction in risk of different strategies for improving awareness of the maritime domain.

The effectiveness of such evaluations, both within and between ports, is influenced to a large degree by the performance standards and goals that are set, as well as the reliability and completeness of the risk assessments that are conducted. To the extent that goals are missing and risk assessments produce data that do not completely and reliably depict threats and vulnerabilities, the prospective evaluation of benefits and costs

[12] See Y. Y. Haimes, S. Kaplan, and J. H. Lambert, "Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling," *Risk Analysis*, Vol. 22, No. 2, 2002, and M. Leung, J. H. Lambert, and A. Mosenthal, "A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks," *Risk Analysis*, Vol. 4, No. 4, 2004.

of future mitigation strategies may not target the areas with the greatest gaps or lead to the most cost-effective decisions.

In examining various alternatives, a key consideration will be measuring the overlapping benefits of different strategies as a means of developing data on what set of alternatives may provide the most improved security in return for the resources expended. These overlapping benefits and costs may involve Coast Guard actions, such as expanding the number of operational centers at port locations or procuring new ships and aircraft, or actions by others, such as more inspections of container cargo shipments or developing better intelligence capability. The Coast Guard's evaluation of alternatives generally involves examining its own possible actions, such as developing proposals to expand the number of operational centers, without placing the cost of such actions in context with other alternatives that have already been deployed or that could be used. In discussions with us, Coast Guard officials said addressing this issue was part of the Coast Guard's efforts to further refine its risk management approach. For example, the Coast Guard is working toward examining alternatives by assessing the degree to which they reduce risk in exchange for the cost involved.

Management Selection: Local Strategies Have Been Selected but Would Be Better Informed by Improvements in Phases for Goal Setting and Risk Assessment

In regard to management selection—the fourth phase of the framework—the Coast Guard has used its port-level assessments to select specific mitigation strategies to manage vulnerabilities in and around facilities. For example, local Captains of the Port have used the assessment information in coordination with input from local stakeholders to (1) establish security zones around key port infrastructures; (2) improve security in and around passenger vessels; and (3) coordinate security improvements, such as fences, cameras, and barriers around port infrastructures. At the national level, the Coast Guard is designing and planning to implement an array of radar systems, sensors, and information systems to identify and track possible threats in the maritime domain. One element of this effort is the establishment of maritime intelligence fusion centers that cover the Pacific and Atlantic coasts. These fusion centers are providing intelligence to the Coast Guard intelligence network in the field, and the centers share information with interagency partners, such as the Navy and Customs and Border Protection.

In general, progress in this area is affected heavily by the same factors affecting progress in evaluating alternatives: progress in setting measurable performance objectives and improving the reliability and completeness of risk assessments. The various phases of the risk management model build and rely on one another, and in this case the quality and reliability of the results are heavily affected by the quality and reliability of efforts in the first two phases.

Another major challenge will be to strategically integrate risk-based data into other management systems, such as the annual cycle of program and budget review for assessing how to deploy resources among ports. Coast Guard officials acknowledged that using risk-based data to inform the annual budget cycle is an important step and are taking further steps to address them. For example, the Coast Guard's MSRAM tool will compare risks at one port with those at another port, and the data produced could inform the Coast Guard's annual budget review of programs and resource allocation. In addition, based in part on our discussions with Coast Guard officials, the Coast Guard's resource planning guide for fiscal years 2008-2012 calls attention to the importance of joining these processes. The guide states that by "employing principles of risk management and using our understanding of strategic risks to Coast Guard mission performance, we will be able to make better decisions regarding investment, re-investment and base management priorities."

Implementation and Monitoring: A Foundation for Continuous Improvement Is in Place; Challenges Remain in Refining It and Developing Formal Policies

The Coast Guard has made progress in the fifth phase of the framework—implementation and monitoring—by improving existing tools and systems in a variety of ways. For example:

- The Coast Guard has improved PS-RAT; version 2, developed in November 2002, by providing such improvements as greater detail on consequence data. Additionally, the MSRAM will include improvements in the quality of threat information in its analysis.
- The Coast Guard used the Port Security Assessment Program to further refine area maritime security plans by offering intelligence and other information to the local Captains of the Port on security issues the plan may not have covered.
- In November 2004, the Coast Guard started conducting the National Maritime Strategic Risk Assessment to obtain comments and feedback from Coast Guard area and headquarters staff on its mission areas, including its port security mission. Among other things, the staff provided input on ways that the Coast Guard could improve the manner in which it carries out its port security mission and reduce any gaps in coverage. For example, staff identified opportunities for leveraging resources, such as strengthening the partnership with

nonfederal stakeholders involved in maritime security, as well as potential gaps in the port security mission, such as training, equipment, and technology. This information was summarized by a Coast Guard consultant and was provided to managers in Coast Guard headquarters.

In some cases, this progress is limited to a degree by a lack of a formal policy for taking action on feedback that is received about ways to improve the risk assessment and management approach. For example, when the Coast Guard receives feedback from field staff on ways to improve its strategic approach, there are no formal policies for addressing the issues raised. Without such policies, there is little assurance that the feedback received will inform decisions to improve risk management practices and ultimately port security. For example, a Coast Guard official at one port noted that while there are informal communication channels to offer feedback on the PS-RAT, there are no formal procedures for doing so, and that such procedures would be useful in addressing concerns of local users when using the tool. Recognizing that there was no formal feedback process for the PS-RAT, the Coast Guard developed an ad hoc methodology to gather feedback from the users of the tool. In March 2005, Coast Guard headquarters hosted a workshop to obtain input from Coast Guard field offices on ways to improve the PS-RAT. The workshop resulted in a list of possible modifications to the PS-RAT and a plan to develop the MSRAM. Coast Guard officials acknowledge that a formal feedback process would be beneficial, and they plan to include one as part of the Coast Guard's MSRAM.

Identifying and addressing organizational barriers to the Coast Guard's ability to improve or carry out its risk management approaches is a final consideration for the monitoring and implementation phase. One key organizational challenge is building and sustaining expertise and skills for effectively designing and using the risk management tools, techniques, and models necessary for managing the Coast Guard's efforts in carrying out its port security and maritime domain awareness responsibilities. The Coast Guard provides training on risk-based decision making at its training center. Recently, the Coast Guard revised its officer evaluation form by including "risk assessment" as a key leadership competency for its officers. Partly on the basis of the briefings we provided to agency officials, the Coast Guard plans to carry out workshops to examine ways to integrate risk management into the PWCS strategic plan and activities. Applying risk management tools and techniques is a complex undertaking, and it requires a managed effort to maintain and build organizational expertise and skills to do the job well.

Conclusions

The foundation the Coast Guard has established for risk management is generally sound. It represents a strong commitment on the Coast Guard's part to using risk management effectively in making decisions. Further, the Coast Guard, often acting on discussions held during the course of this review, has actions under way to address many of the concerns we identified. The most difficult work ahead revolves around systematically integrating risk-based information into management systems, including the annual cycle of program review, that can help inform decisions about how to deploy resources and security measures among ports and to examine the value of new programs in addressing security gaps that remain. In this regard, the Coast Guard's efforts are still in the early phases of development. As the Coast Guard moves forward, it is especially important that the agency develop ways to establish a stronger linkage between the various local and national risk assessment efforts under way. For example, area maritime security plans are not comparable, and security risks at one port location cannot be compared with the risks identified at another location. As a result, the collective value of these individual efforts is diminished. Developing ways to establish a stronger linkage would likely increase the value of the work.

Recommendations for Executive Action

We are not making recommendations in those areas where the Coast Guard has actions well under way. The recommendations below are designed primarily to spotlight those areas in which additional steps are most needed to strengthen agency efforts to implement a risk management approach to the Coast Guard's port security activities. Accordingly, we recommend that the Secretary of Homeland Security direct the Commandant of the Coast Guard to take action in the following two areas:

- *Risk assessment*: Develop plans to establish a stronger linkage between local and national risk assessment efforts. This effort could involve strengthening the ties between local assessment efforts, such as area maritime security plans, and national risk assessment activities.

- *Alternatives evaluation and management selection*: Ensure that procedures for these two processes consider the most efficient use of resources. For example, one approach involves refining the degree to which risk management information is integrated into the annual cycle of program and budget review.

Agency Comments and Our Evaluation

In commenting on a draft of chapter 2, DHS, including the Coast Guard, generally agreed with our findings and recommendations. DHS said that the report notes that the Coast Guard has made progress in all five risk management phases and is taking action to address the challenges that remain. In addition to commenting on our recommendations, the Coast Guard provided several technical comments under separate cover, and we revised the report when appropriate. Written comments from DHS are in appendix II.

Chapter 3: Stronger Risk Management Approach Could Improve the Accountability of the Port Security Grant Program

The Office for Domestic Preparedness within the Department of Homeland Security has made progress in applying risk management to the port security grant program but faces challenges in strengthening its approach, as demonstrated in part by its experience in awarding past grants. Examples of progress—and challenges—can be found across all five risk management phases (see table 6). ODP has established overall goals for the grant program but faces challenges in setting specific and measurable program objectives, in part because this effort hinges on similar action by other federal agencies. ODP's progress, with input from the Coast Guard and IAIP, has been greatest in conducting the actual risk assessments. It assessed 129 ports and, using risk-based prioritization, narrowed to 66 the number of ports eligible to apply for fiscal year 2005 grants. Its methods for assessing risks and evaluating mitigation alternatives, however, still are limited in their ability to prioritize relative risks across ports or to calculate the costs and benefits of various alternatives. Finally, while ODP has also made progress in developing a risk-based grant selection process and mechanisms to monitor what the grants accomplish, it has not always completely relied on a risk-based process. For example, grant awards for fiscal year 2004 illustrate the trade-offs that occur when attempting to award grants to applicants that are at greater risk and, at the same time, provide funds to applicants that have the larger financial need. At the end of what was, in part, a risk-informed assessment process, ODP change the criteria for awarding grants when it decided to give lower priority to grant applications involving projects at large companies, on the assumption that these companies were better able than other entities to pay for their own security improvements. This changed 40 percent of the grants originally recommended for an award, as projects with higher risk but greater potential for self-funding gave way to lower-risk projects with more limited funding prospects. ODP changed the process for fiscal year 2005 by clarifying the criteria it would use in awarding grants and by requiring applications from private entities to match at least 50 percent of the total amount requested.

Table 6: Summary of Progress and Challenges in the Port Security Grant Program

Risk management phase	Examples of progress made	Examples of remaining challenges
Strategic goals, objectives, and constraints	High-level strategic goals have been set for the port security grant program.	The program is missing measurable program objectives to show the progress that has been made.
Risk assessment	In its May 2005 guidelines, ODP has prioritized spending decisions by identifying 66 key seaports that are eligible for awards, and it is placing greater reliance on the use of risk assessments at port locations.[a]	Threat, vulnerability, and consequence data have limitations. The degree to which risk assessments compare and prioritize risk across ports remains a challenge.
Alternatives evaluation	Unlike efforts in previous years, the fiscal year 2005 effort examined alternative solutions proposed by nonfederal stakeholders and ODP, and the Coast Guard assessed the cost and benefits of the projects.	The degree and extent to which proposals can be accurately evaluated and benefits calculated for risk reduction remains uncertain. ODP is working with the Coast Guard to deal with this challenge.
Management selection	For fiscal year 2005, criteria for management selections include the prioritization of projects based on the criticality of ports and proposals that reduce vulnerabilities to certain threat scenarios. These risk-based criteria were not used in prior fiscal years.	For fiscal year 2004, internal controls for documenting management decisions were not followed. For fiscal year 2005, ODP documented grant award decisions in a database.
Implementation and monitoring	In fiscal year 2005, ODP has made a number of improvements to better monitor implementation of its risk management process.	For fiscal year 2004, additional improvements were needed to obtain formal feedback from grant program stakeholders. For fiscal year 2005, ODP has developed formal feedback loops from grant program stakeholders.

Source: GAO analysis of ODP's port security grant program.

[a] The Coast Guard provided various data on ports, such as amount of total cargo, domestic cargo, international cargo, number of passengers using ferries, and number of passengers using cruise ships. ODP prioritized ports by evaluating these data to determine a list of the 66 highest-risk port areas.

ODP Manages Port Security Grants

The port security grant program was established in fiscal year 2002 under the purview of the Transportation Security Administration (TSA), which became part of DHS in March 2003.[1] Because of organizational changes within DHS, the grant program has been administered by ODP within the Office of State and Local Government Coordination and Preparedness

[1] The legislation enabling the port security grant program was the Department of Defense and Emergency Supplemental Appropriations for Recovery from and Response to Terrorist Attacks on the United States, 2002, Pub. L. No. 107-117, 115 Stat. 2230, 2327 (2002).

since May 2004. ODP was transferred from the Department of Justice to DHS upon passage of the Homeland Security Act of 2002.

The grant program provides assistance to nonfederal stakeholders for making security improvements at the nation's ports. During fiscal years 2002-2004, grants from the program totaled about $560 million and covered such concerns as more fencing, cameras, and communications equipment. For fiscal year 2005, the appropriations act for DHS provided $150 million for port security grants.[2] The 2005 program focused on three primary concerns: (1) protection against improvised explosive devices carried by small craft, underwater craft, or vehicles; (2) enhanced explosives detection capabilities for the owners and operators of vehicle ferries and associated facilities (as shown in fig. 3); and (3) facility security enhancements in the nation's highest-risk ports. The program is designed to operate in coordination with federal partner agencies and industry.[3] Grantees are selected through a competitive process.

[2] Department of Homeland Security Appropriations Act, 2005, Pub. L. No. 108-334, 118 Stat. 1298, 1309 (2004).

[3] Federal agency and industry partners include the United States Coast Guard, the Information Analysis and Infrastructure Protection Directorate, the Border and Transportation Security Directorate, and the Transportation Security Administration within DHS; the Maritime Administration within the Department of Transportation; and the American Association of Port Authorities.

Figure 3: Facilities at One of the Nation’s Major Ports

Source: GAO.

For fiscal year 2006, the Office of Management and Budget had proposed consolidating the port security grant program with other homeland security grant programs. Known as the Targeted Infrastructure Protection Program, the program would have consolidated funding for ports, transit, and other critical infrastructure into one program. However, DHS's appropriations act for fiscal year 2006 maintained separate funding for the port security grant program. In particular, the act provided a $175 million appropriation for the port security grant program that, "shall be awarded based on risk and threat."[4]

In January 2005, the DHS Office of the Inspector General issued a report on the Port Security Grant Program that covered the program’s second and third rounds of grants—through fiscal year 2003.[5] This report made a number of recommendations, and in response, ODP initiated a number of

[4] Department of Homeland Security Appropriations Act, 2006, Pub. L. No. 109-90, 119 Stat. 2064, 2075 (2005).

[5] Department of Homeland Security, Office of Inspector General, *Review of the Port Security Grant Program*, OIG-05-10 (January 2005). In some years, more than one round of grants has been awarded. In all, five rounds of grants were awarded between 2002 and 2005.

changes to the program, according to ODP grant program officials. Our discussion of the grant program reflects the changes ODP had made at the time of our report.

Goal Setting: Overall Goals Have Been Set; Developing Performance Measures and Leveraging Federal Dollars Remain Challenges

Progress has been made on setting goals—the first phase of GAO's risk management framework—for the port security grant program. Congress and the Administration have laid out broad policy goals for maritime security and for the program. Congress's stated purpose in establishing the program was to finance the costs of enhancing facility and operational security at critical national seaports.[6] The Administration has set the program in the context of the December 2004 Presidential Directive on Maritime Security Policy, which cites several broad policy goals for maritime security, including preventing terrorist attacks in the maritime domain and reducing vulnerability to such attacks; protecting U.S. population centers, critical infrastructure, borders, harbors, ports, and coastal approaches; and maximizing awareness of security issues in the maritime domain in order to respond to identified threats.[7]

DHS's application guidelines for fiscal year 2005 grants reflect the context of these broad policy goals. They state that the program reflects congressional and executive intent "to create a sustainable effort for the protection of critical infrastructure from terrorism, especially explosives and nonconventional threats that would cause major disruption to commerce and significant loss of life," and they link the program to specific national priorities specified in the nation's security planning framework.[8] Other ways in which the 2005 grant program reflects a goal-oriented approach are its efforts to apply the grants to locations that are viewed as the nation's highest-risk ports (discussed in more detail below) and to focus the grants on such specific concerns as protection against improvised explosive devices.

[6] The Department of Defense and Emergency Supplemental Appropriations for Recovery from and Response to Terrorist Attacks on the United States, 2002, Pub. L. No. 107-117, 115 Stat. 2230, 2327 (2002).

[7] Homeland Security Presidential Directive 13 (Dec. 21, 2004).

[8] Office for Domestic Preparedness, U.S. Department of Homeland Security, *Fiscal Year 2005 Port Security Grant Program: Program Guidelines and Application Kit* (Washington, D.C.: 2005). The specific national priorities cited are (1) chemical, biological, radiological, nuclear, and explosive detection and response capabilities and (2) National Infrastructure Protection Plan implementation.

While broad policy and program goals have been set, challenges to further progress on this risk management phase take two main forms. The first is translating the program's broader goals into measurable objectives. One difficulty in doing so is that other federal partner agencies have yet to spell out measurable objectives at the national level as related to protecting key infrastructure. For example, as discussed in chapter 2, the Coast Guard's Maritime Strategy for Homeland Security describes strategic approaches and priorities, but it does not include measurable objectives as part of its approach.[9] In addition, DHS has yet to set performance measures for programs related to the implementation of programs for protecting critical infrastructures—another program area that the grant program supports.[10] We discuss this further in chapter 4.

A second challenge involves determining an appropriate way to consider two different federal concerns about grant programs: ensuring that grants address key needs while at the same time ensuring that they make the most efficient use of federal dollars. This challenge exists for several reasons:

- *Federal and nonfederal partnership for addressing key needs.* First, the federal government is not the only potential source of revenue for addressing security needs. Ports are often a complex mixture of public sector and private sector infrastructure. For example, public entities such as port authorities or local and state governments may own or operate seaport facilities and roadways, while private companies and interests may own and operate factories, warehouses, oil refineries, and railways.[11] Ports can produce benefits that are public in nature (such as general economic well-being) and distinctly private in nature (such as generating profits for a particular company). The public benefits they produce can also be distinctly local in nature, such as sustaining a high level of economic activity in a particular state or metropolitan area. Thus, state and local governments, like private

[9] *U.S. Coast Guard: Maritime Strategy for Homeland Security*, (Washington, D.C.: December 2002).

[10] In some ways, owners and operators of facilities and vessels have set their own standards for what an acceptable level of risk is by the security plans they have developed under the Maritime Transportation Security Act of 2002. As required by the act, 46 U.S.C. 70103(c), facility and vessel owners developed over 12,000 plans to reduce vulnerabilities around their port areas. The Coast Guard required facility and vessel owners to implement them by July 1, 2004.

[11] ODP estimates that 90 percent of facilities and vessels are owned by industry.

companies, also have a vested interest in ensuring that their ports can act as efficient conduits of trade and economic activity. Given that homeland security threats can imperil this activity, it can be argued that all of these stakeholders should invest in the continued stability of the port.

- *Leveraging federal dollars.* Second, in many federal grant programs, the desired outcome is that federal grants *supplement* what other stakeholders are willing to spend. If a grant program is not designed to encourage supplementation, the danger is that other stakeholders will rely solely on the federal funds and choose to use their own funds for other purposes. This practice is known as substitution, and the net result is that limited federal funds cannot be stretched, or leveraged, to the degree they otherwise could be. In prior work addressing this issue in certain other grant programs, we found that on average, every additional federal grant dollar resulted in about 60 cents of substitution.[12]

Although the design of a grant program is not part of the risk management framework, it is an important issue because it is one key to accomplishing the dual aims of targeting funds to projects that address the highest risk while discouraging the replacement of state, local, and private funds with federal money. ODP's approach for 2005 has been to formalize a matching requirement for private sector stakeholders but not for public sector stakeholders. For fiscal year 2005 grants, ODP required that applications from industry match at least 50 percent of the total amount requested.

This situation illustrates the complexity of addressing the most significant security needs while considering the degree to which nonfederal stakeholders should share in the cost of security improvements. For fiscal year 2005, the program encourages but does not require public sector or

[12] GAO, *Federal Grants: Design Improvements Could Help Federal Resources Go Further*, GAO-AIMD-97-7 (Washington, D.C.: Dec. 18, 1996). We include this figure here for illustrative purposes only and are not stating that this degree of substitution would occur in the port security grant program. For discussion of this issue in other public/private arenas, such as federal funding for highway investments and freight mobility projects, see GAO, *Freight Transportation: Strategies Needed to Address Planning and Financing Limitations*, GAO-04-165 (Washington, D.C.: Dec. 19, 2003); *Highway and Transit Investments: Options for Improving Information on Projects' Benefits and Costs and Increasing Accountability for Results*, GAO-05-172 (Washington, D.C.: Jan. 24, 2005); and *Freight Transportation: Short Sea Shipping Option Shows Importance of Systematic Approach to Public Investment Decisions*, GAO-05-768 (Washington, D.C.: July 29, 2005).

nonprofit entities to match federal funds, according to ODP officials. Depending on the value placed on reducing the substitution of federal funds for local funds, the design of the port security grant program offers a way to improve the fiscal impact of federal dollars. There is disagreement among policymakers about where the emphasis should be on this aspect of grant programs. Some might see the substitution of federal funds for local funds as reasonable given differences in fiscal capacity, while others may view homeland security as a shared fiscal responsibility. If policymakers place greater value on reducing the substitution of federal funds for local funds, strengthening matching requirements for such entities offers one option. The 2006 appropriation for the port security grant program includes a federal matching requirement.[13] ODP has not yet issued its 2006 port security grant guidance clarifying how it will implement this requirement. One way to implement the requirement involves using a sliding scale for matching federal funds depending on the fiscal capacity of the grant applicant. Such a scale could range, for example, from an 80 percent matching requirement for Fortune 500 companies to a 25 percent matching requirement for those entities that have less in monetary resources.[14]

Risk Assessments: The Funding Distribution Model Is Becoming Better Able to Consider Risk, but Methodological Challenges Remain

ODP has made progress in carrying out risk assessments—the second part of the risk management framework—but the progress made is balanced by the additional methodological challenges that remain. ODP's progress is reflected in changes made to the program for fiscal year 2005, in both port-level and national-level assessments. Among other things, ODP has placed greater emphasis on using threat, vulnerability, and consequence data in prioritizing applications and port locations. Nonetheless, various methodological challenges remain in the assessment tools or the assessments themselves. For example, ODP is still limited in its ability to compare and prioritize applications from one port with those from a different location.

[13] Department of Homeland Security Appropriations Act, 2006, Pub. L. No. 109-90, 119 Stat. 2064, 2075 (2005). The appropriation incorporates by reference the federal matching requirement of another federal grant program contained at 46 U.S.C. 70107(c). The match provision allows federal funding up to 75 percent of the total cost of the project, unless the DHS Secretary determines that a proposed project merits support and cannot be undertaken without a higher rate of federal support.

[14] *Fortune* magazine ranks the nation's largest companies on the basis of revenue.

Procedures for the Fiscal Year 2005 Port-Level and National-Level Assessments Have Been Strengthened

At the port level, a key difference in ODP's fiscal year 2005 grant procedures is that input from other stakeholders plays a more prominent role in the award decisions. ODP obtained such input in prior years but did not formally consider it in making decisions. For example, in making its determinations for fiscal year 2004 grants, ODP sought input from the Coast Guard Captains of the Port and from regional directors of the Maritime Administration. These officials reviewed and ranked port security grant applications based on their knowledge of the port location and the results of various assessments, including the PS-RAT. ODP officials said they considered this input, but they did not integrate rankings into the evaluation forms used in the ODP assessment process. In this regard, the DHS IG found that ODP should place greater emphasis on risk reduction as part of the grant review process.[15] In responding to the IG's findings, for fiscal year 2005, the rankings made by Coast Guard, Maritime Administration, and state officials are part of the formula ODP uses to make final decisions on grant awards.[16] Additionally, the 2005 program places greater emphasis on applications that are consistent with area maritime security plan priorities.

ODP's adjustments to its fiscal year 2005 procedures are even greater at the national level, where it has made a concerted effort to narrow the program to ports of greatest concern, and to use threat, vulnerability, and consequence data to rank and prioritize both ports and applications. For grants made in fiscal year 2004, ODP considered applications from all ports in making awards. For the 2005 program, ODP worked with IAIP and the Coast Guard to develop a list of eligible ports. The agency first identified the largest ports based on volume. According to ODP officials, a risk formula was developed to rank each of the ports. In May 2005, ODP determined that, on the basis of this assessment, 66 of the 129 largest-volume ports across the country were eligible for grant awards.[17] ODP

[15] Management for the fiscal year 2004 program was transferred from the Transportation Security Agency to ODP during the middle of the process. ODP assumed full responsibility for the program in fiscal year 2005.

[16] For the 2005 program, the evaluation at the port level is managed by the Coast Guard Captain of the Port and state officials when feasible. Applications are reviewed against established criteria and ranked on relative risk, with the highest rank going to applications that support the national port security priorities.

[17] ODP defines risk as credible threats and incidents (from the intelligence community), less credible threats and incidents (operational indicators), and vessels of interest. It defines vulnerability as distance from open water, number of port calls, and presence of tankers, and it defines consequence as people, economic, national security, and port-specific special considerations (such as hazardous materials or oil).

further prioritized the 66 ports by dividing them into four tiers—tier 1 representing those ports with the highest risk and tier 4 representing ports with the lower risk. ODP provided a set amount of money to each tier, and ports in these tiers competed against each other for funding. In carrying out its analyses, ODP also placed greater reliance on threat, vulnerability, and consequence information.

Beyond reducing the number of ports eligible for the grant program, another change ODP made at the national level was to prioritize possible threat scenarios that grant funds should address, using input from Coast Guard officials. ODP has given priority to applications that prevent or detect threats arising from improvised explosive devices. Such devices pose a threat to transportation systems across the nation and have been used by terrorists in the past. Specifically, for the 2005 grant program, ODP has given priority to the following threat scenarios:

- preventing and detecting improvised explosive devices delivered via small craft,
- preventing and detecting underwater attacks from such devices, and
- preventing and detecting vehicle-born improvised explosive devices on ferries.

Challenges Remain for Improving Methods and Data

ODP's assessment methodology, while improved, still faces challenges. Progress in using risk assessment data to manage the grant program has limitations in methods and data for informing award decisions. These challenges, if addressed, would provide decision makers with more reliable and complete data on which to prioritize and award grant funds. The challenges fall into two main categories: (1) incomplete threat, vulnerability, and consequence data and (2) methodological inability to fully compare grant applications from one port with those from another port.

Incomplete Data on Threats, Vulnerabilities, and Consequences

Our review of ODP's risk assessment approach and our discussions with ODP and Coast Guard personnel identified several challenges related to data on threats, vulnerabilities, and consequences (see table 7).[18] Many of

[18] Although ODP has primary responsibility for administering the grant program, the Coast Guard plays a key role in the program. Local Captains of the Port use the PS-RAT in evaluating grant applications at the local level, and ODP officials consult frequently with Coast Guard officials at the national level.

these challenges mirror the challenges faced by the Coast Guard that we described earlier in chapter 2.

Table 7: Examples of Data-Related Challenges in ODP Risk Assessments

Data type	Summary of challenge
Threats	Data on threats provide a useful starting point. However, ODP is challenged, just as the Coast Guard is, in conducting risk assessments without data on the relative likelihoods associated with various threat scenarios. Information from the intelligence community on such things as the presence of national or international terrorist cells, and on the capability and intent of terrorist groups as they relate to types of scenarios and the specific infrastructure type, would enhance ODP's ability to model relative probabilities of threat scenarios.
Vulnerabilities	ODP's assessment of vulnerabilities does not take into account actions that have already been taken to reduce vulnerabilities (such as more patrols, fencing, and guards). While ODP has prioritized certain scenarios, the vulnerability assessments are not linked to specific threat scenarios, thus limiting the value of vulnerability scores.
Consequences	Similar to its assessment of vulnerabilities, ODP's assessments of consequences are not linked to specific threat scenarios. Instead, ODP uses values such as population density near a port or cargo tonnage to measure consequences.

Source: GAO analysis of ODP's risk assessment for the port security grant program.

The following examples illustrate the challenges posed by the limitations in threat, vulnerability, and consequence data.

- *Limitations in threat-related data.* ODP's current characterization of threat cannot be interpreted as an estimate of relative probability of threat scenarios—a key element of risk assessment—in and around ports.[19] The problems we pointed out in chapter 2 about threat data are applicable here as well: The threat information available from intelligence agencies does not provide the type of data that could be used to more fully inform ODP's decisions. More complete data would include such things as information on the presence of national or international terrorist cells, the capability and intent of terrorist groups as they relate to types of attack, and on the specific infrastructure types that have been attacked. ODP officials said that the scarcity of threat data limits their ability to inform the decision-making process and that decisions are based on the best available combination of data and expert judgment. Because threat data are limited, ODP bases its models on several proxies for risk. For example, ODP used volume of cargo that moves into and out of ports as a way to develop its list of the 129 ports that could initially be candidates for the grant program. ODP

[19] ODP relied on threat-related information provided by IAIP for the fiscal year 2005 grant program.

then assessed the relative risk at these ports by using, among other things, a threat variable represented by the number of "credible threats and incidents" and the number of "vessels of interest" (i.e., suspicious vessels) that use a port facility. These data originated from the intelligence community, the Coast Guard, and IAIP. ODP recognizes, however, that threat data on ports are scarce, and data on the number of credible threats and incidents and vessels of interest may not represent actual threats, but instead could also represent other law enforcement problems, such as illegal migrants or theft of goods and merchandise. The challenges in developing reliable data on probability affect the overall risk assessment for a port area, given a specific attack scenario. Without data or models that measure the relative probability of various threat scenarios, ODP may not target the most significant security concerns.

Limitations in vulnerability-related data. As we described in chapter 2, the Coast Guard's PS-RAT excludes from its analysis reductions in vulnerabilities resulting from security measures that have already been taken by the Coast Guard, such as inspecting passenger vehicles that board ferries, escorting high-interest vessels, and establishing security zones around the port. ODP's assessment of vulnerabilities involves specific aspects of individual port areas themselves, namely, data on the length of the channel leading to a port, the number of port calls by all ships, and the number of tankers that use a port. While such data are representative of the intrinsic vulnerabilities of a port's location, they do not include such factors as guards, fences, and cameras that are already in place; security zones that have been established; or escorts of high-interest vessels that occur. As a result, the assessment may overstate vulnerabilities for port locations. Also important is the fact that ODP's approach to evaluating port area vulnerabilities excludes consideration of specific threat scenarios. For example, while they have identified certain threat scenarios as priorities, the vulnerability indicators are not linked directly to scenarios, such as the use of improvised explosive devices. Without this linkage to the threat component of the risk assessment process, ODP's approach to vulnerability assessments may not consider certain factors, such as the number of areas in a port location where recreational vessels are unmonitored, and how such factors may be conducive to certain threat scenarios, such as loading improvised explosive devices on such vessels.

Limitations in consequences-related data. The values used by ODP to describe the consequences of a terrorist attack may not accurately depict the damages resulting from a terrorist attack. In valuing the consequences of an attack, ODP focuses on people-related, economic-related, and national security-related measures.[20] For example, ODP uses maximum population density within 10 miles of a port and the average number of daily ferry passengers to estimate the consequences of a terrorist attack at a port, and it aggregates these measures. Similarly, ODP uses international and domestic tonnages, the amount of containerized cargo, and the dollar value of foreign trade to measure the economic consequence of a terrorist attack. While these provide a useful starting point, there are two issues related to this approach. First, without linking these data to the relative probability of various threat scenarios, ODP's estimate of consequences is limited to inherent characteristics of a port rather than the estimated consequences of various attack scenarios. In contrast, agencies such as the Coast Guard estimate the number of lives lost and assign a dollar value to the loss of human lives. Second, ODP aggregates the estimated number of lives lost with the dollar value of foreign trade. Doing so raises questions about the reliability and meaning of the final output.

Methodological Limitations

As was the case with the Coast Guard, a key methodological limitation affects one goal of risk assessments—informing decision makers on relative risks across port locations. This limitation relates directly to the ability to compare the relative risks of facilities at one port with those at another port. When field review teams rank and prioritize grant applications, they use several sets of data, including information provided on the application, personal knowledge of the port, and the results of the PS-RAT, which gives ranking information for a given port area on vulnerability and consequence.[21] As discussed in chapter 2, PS-RAT, however, cannot now be used to compare the risks at one port with those at another. PS-RAT allows ODP to compare and prioritize key infrastructure within a port, but it does not produce a risk ranking that permits ODP to compare and prioritize infrastructure across ports. Coast

[20] ODP worked with the Coast Guard and IAIP in developing the consequence measures.

[21] When the port security grant program was established, according to a program official, it was one of the first programs to use the PS-RAT in order to identify risks. The PS-RAT has been very useful on the local level as a means for the Coast Guard to look at relative risk to assets within a port zone in a systematic way. In addition to being a primary tool for the port security grant program, the PS-RAT has also been used by members of the Area Transportation Security Committees to interact with one another and to plan their work.

Guard efforts to develop a tool that examines relative risks across ports will aid ODP in addressing this limitation.

Alternatives Evaluation: ODP Recognizes the Importance of Evaluating Alternatives, but Tools for Doing So Are Limited

Evaluation of alternatives—the third phase of GAO's risk management framework—is an area that ODP recognizes as being an important part of awarding grants, and the changes for fiscal year 2005 represent progress in this area. One change for fiscal year 2005 involves additional steps to consider benefits and costs. When ODP asks local Coast Guard Captains of the Port to review applications, one criterion it asks them to apply is which projects offer the highest potential for risk reduction for the least cost. For 2005, ODP plans to augment evaluation by conducting an analysis of costs and benefits of the project (which considers the potential for risk reduction), and it shares the results with the Coast Guard.

As part of this assessment, ODP plans to break out applications from the 66 eligible port locations into four tiers and give applications from ports that are in higher tiers more priority and more money. Port areas with the highest risk are assigned to tier 1 and port areas with the lowest risk are assigned to tier 4.

ODP's ability to assess proposed security improvements, like the Coast Guard's, is influenced by the program goals and performance measures that the component sets and the reliability and completeness of the risk assessments that it carries out. However, when measurable objectives are missing, the degree to which security gaps remain and the extent to which progress has been made remain unclear. Similarly, while PS-RAT provides a starting point for evaluating the proposed measures and the extent to which the measure narrows security gaps within a port, it was not designed to compare and prioritize relative risks from one port to relative risks in a different port. This condition limits ODP's ability to compare the benefits of proposed security measures from an applicant at one port location with benefits of proposed measures at a different port.

Management Selection: ODP Has Addressed Problems in Documenting Differences between Initial Selection Recommendations and Final Selection Decisions

Earlier in this chapter, we discussed the importance—and difficulty—of balancing potentially conflicting goals, such as ensuring that funds are directed to projects of the greatest risk while at the same time stretching limited federal dollars to the maximum degree. ODP's selection of grants for 2004 illustrates the challenges in applying a risk-based approach to awarding grants and the trade-offs involved in attempting to balance risk and financial need as criteria. In order to achieve accountability, federal standards for internal controls require that all transactions and other major events need to be documented. Basically, about 40 percent of ODP's final selection decisions were different from the initial recommendations of lower-level evaluators, without documentation from reviewers explaining why they disagreed with the initial recommendations. According to officials involved in the program, before the final selections were made, the Secretary of Homeland Security issued guidance indicating that Fortune 500 companies should be able to pay for their own security improvements and that ferries and port authorities should receive higher priority in the final award decisions than other applicants. ODP officials said that the fact that they followed this new guidance affected the final ranking of grant applicants. The tension between self-funding and security priorities illustrates the need for effective internal controls to ensure that procedures are followed and that the resulting selection decisions are transparent and clearly documented. ODP has taken action to address this problem.

In the 2004 grant award process, ODP's initial assessments resulted in recommendations for funding 154 specific proposals.[22] However, our analysis of the final grant awards showed that about 40 percent of the initial 154 applications that were recommended for a grant award by lower-level evaluators that examined grant applications did not receive an award. Table 8 shows examples of the types of changes that occurred.

[22] ODP worked with TSA staff during the assessment process.

Table 8: Examples of Changes in Funding Decisions

Examples of projects initially recommended for funding but ultimately not approved
One applicant requested grant funds to improve security involving the construction of two main entrance access barricades, perimeter lighting, and additional cameras. The applicant offered to share costs—about 20 percent of the $468,000 that it was requesting. After its initial review, ODP staff ranked this application as the third highest and recommended it for an award. The final decision ranked this applicant 228 out of 287 applicants, and the application did not receive an award. According to staff familiar with this project, the applicant received a lower ranking because it was a Fortune 500 company.
Another applicant requested $225,000 in grants to purchase cameras, fencing, and barricades around its facility, and it committed to matching the requested amount. The initial headquarters review recommended that the applicant receive an award and it ranked the project as 25th out of 287 applicants. Local Coast Guard and MARAD officials ranked this project as their top priority for the port, noting that this chemical plant produces material that is highly hazardous and that improving security at this facility had the Coast Guard's "highest recommendation." This applicant did not receive an award and it was ranked 236 out of 287 applications because it was a Fortune 500 company.
Examples of projects initially not recommended for funding but ultimately approved
Another applicant requested a $1.1 million grant to augment an existing police department surveillance and camera system of port facilities on an around-the-clock basis. The initial headquarters review did not recommend this application for an award and it was ranked 279th out of 287 applicants. Comments from the initial review showed that there was concern the project was not cost-effective because "it appeared to duplicate another effort by the port or the state and the project provided moderate risk reduction to identified vulnerabilities." The reviewers noted that the applicant did not offer to share in the cost of the project. However, ODP awarded $800,000 to the applicant.
A fourth applicant requested $1,105,200 to install protective film on windows at its terminal location. Grant program procedures stated that preference would be given to projects that prevent, deter, and detect (an attack) over a project that involved new installation or replaced existing infrastructure. On the basis of these guidelines, the Coast Guard staff at one port location ranked this application as 50th out of 55 applicants in its port zone. According to the staff, they were instructed to raise the scores for this application, and as a result, the applicant received an award for its application.

Source: GAO analysis of 2004 grant fund database.

These examples illustrate the trade-off between awarding grants to applicants that are assessed, in part, based on risk or on providing funds to applicants that have a financial need. The net result is that when federal funds are used in this fashion, they may not address the most severe security gaps in and around ports because there is no guarantee that private sector firms will spend their own funds for security improvements since it is unclear whether there are incentives, such as minimum standards for security, that would motivate them to do so.[23] The competing goals of addressing the most significant security needs and providing financial assistance to those entities with less fiscal capacity call attention to the difficulty of achieving a balance between these objectives and the need for selection decisions that clearly document the trade-off.

In order to achieve a transparent process for accountability purposes, federal standards for internal control require that all transactions and other significant events need to be clearly documented, and that documentation should be readily available for examination.[24] However, internal control procedures for documenting decisions, including changes in project ranking, were not followed. The result is that the rationale for award decisions was not always available. In cases where an applicant's ranking would change by over 100 places, there was no documentation that described the reason for the change. In several cases where changes such as this occurred, it was noted that the final selection board concurred with the original ranking, but no reason was provided for the reprioritization. DHS's IG review also found this lack of documentation. The IG recommended that the reviewers be required to document their decisions in the grants management system, particularly when the decisions are inconsistent with recommendations from a lower level of review. DHS generally concurred with the IG's recommendations and stated that it would require reviewers to document their decisions as part of the 2005 grant program. Our work showed that in the fiscal year 2004 grant program—the most recent round prior to the issuance of the IG's report—such documentation was still missing. For fiscal year 2005, ODP instituted additional measures to ensure that decisions were documented as part of the review process.

[23] MTSA required owners and operators of facilities and vessels to develop and implement security plans by July 1, 2004. In all, about 12,300 plans were developed. The Coast Guard is charged with approving the plans and ensuring owners and operators are complying with the actions called for and determining whether all vulnerabilities have been identified. Coast Guard compliance inspections were scheduled for completion by July 2005. Funds requested by owners and operators may reflect additional security measures taken that go beyond the minimum requirements called for in the security plans or they could involve additional technology improvements.

[24] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

Implementation and Monitoring: ODP Has Instituted a Monitoring Plan for Grant Awards

ODP has made substantial progress in creating procedures that address the fifth phase of the framework—implementation and monitoring; the challenge lies in carrying them out. As we have described in this chapter, ODP has taken a number of actions to base spending decisions on risk-based data; it has, among other things, (1) developed procedures for prioritizing port locations, (2) prioritized threat scenarios, and (3) more closely aligned risk assessments to port locations. In addition, ODP has coordinated its efforts with the Coast Guard, the intelligence community, and other key stakeholders in developing the procedures for the 2005 grant program. For the fiscal year 2005 grant program, ODP has established procedures for monitoring recipients after they have been funded. The monitoring consists of follow-up after a project has been implemented to help ensure that the project has been implemented in accordance with the grant award, including timelines, budgets, and programmatic criteria are being met. In addition, ODP requires that progress reports be submitted biannually and a final project report be submitted within 120 days after the end of the project.

A challenge that remains this phase of the risk management framework is developing processes for feedback to improve the process used in awarding grants. For example, our review of the 2004 grant awards show that local officials, including Coast Guard officials and grant applicants, did not receive feedback from ODP on why projects they designated as high priority did not receive funding when lower-priority projects did. According to ODP officials, they have instituted processes for providing feedback to and obtaining feedback from grant program stakeholders as part of the fiscal year 2005 program.

Conclusions

The principles of risk management apply to the port security grant program, and the lessons learned call attention to additional actions that could build on the progress that has already been made. Depending on the value placed on reducing the substitution of federal funds for local funds, there are opportunities to further leverage federal dollars in the program's design, and by leveraging federal funds, additional security needs in and around ports could be addressed. Additionally, without having performance measures in place, it is hard to gauge what progress has been made and what security gaps remain. The development of such measures should offer greater insights on the extent to which funds are narrowing security gaps that exist or helping to identify security needs that surface. The lessons of the program also provide numerous insights into the way that multiple stakeholders, such as the Coast Guard and IAIP, contribute to the way in which ODP uses risk-based data in administering the program. As we described in chapter 2, the Coast Guard has several efforts under way to improve its risk assessment of ports, including developing data on the relative probability of threat scenarios, improving data on consequences and vulnerabilities that are linked to various threat scenarios, and comparing risks among ports. ODP should be able to use the results of such efforts to help in awarding grants that are consistent with the priorities identified.

Recommendations for Executive Action

To strengthen ODP efforts to implement a risk management approach to its port security grant program, we recommend that the Secretary of Homeland Security direct the Executive Director for ODP to undertake the following three actions:

- Clarify, in its grant guidance, the conditions under which greater leveraging of federal dollars should be included as a strategic goal for the port security grant program.
- Develop measurable objectives for managing the grant program's progress toward achieving strategic goals and use these measures to gauge progress and make adjustments to the program.
- Coordinate efforts with the Coast Guard and IAIP to use more reliable risk assessment data as they become available. At a minimum, such data should include (1) the relative likelihood of various threat scenarios, (2) consequences and vulnerabilities that are linked to terrorist scenarios, and (3) a comparison of risks across ports.

Agency Comments and Our Evaluation

In commenting on a draft of chapter 3, DHS, including ODP, generally agreed with the findings and recommendations. Specifically, DHS said that the recommendations are reasonable given that most of our review took place prior to changes that ODP made to the program in fiscal year 2005. DHS said that it appreciated our efforts to review the fiscal year 2005 port security grant program requirements even though most of our work had been completed. DHS stated that several of the recommendations have already been addressed, and it noted that the remaining ODP-related recommendations will be addressed in the fiscal year 2006 port security grant program, at least to the extent possible. In addition to commenting on our findings and recommendations, DHS provided technical comments under separate cover, and we revised the draft report where appropriate. Written comments from DHS are in appendix II.

Chapter 4: IAIP Faces Challenges in Meeting Risk Management Responsibilities across All Sectors of the Nation's Infrastructure

The Information Analysis and Infrastructure Protection Directorate within DHS faces broad and extensive challenges in meeting its risk management responsibilities and thus far has made limited progress. Relative to the Coast Guard and ODP, IAIP's risk management responsibilities are much wider and more difficult: Instead of comparing risks across port assets, it must find ways to compare risks at ports with risks in other sectors, such as public health, energy, and banking and finance. Challenges remain across all of the phases of GAO's risk management framework (see table 9). For the first phase (goals and objectives), while IAIP's efforts are anchored to strategic goals in various executive branch strategies and an interim national plan, IAIP's challenge is to continue developing the national plan to provide performance measures and associated steps and milestones. In the second phase, IAIP has begun several key risk assessment efforts but has had limited success in completing them. For example, IAIP faces challenges in developing data on the relative likelihood of various threat scenarios—a key part of the assessments it must conduct under the Homeland Security Act of 2002—because the information produced by the intelligence community is of limited use for risk assessment purposes, according to IAIP officials. IAIP has plans to develop such data by coordinating its efforts more closely with the intelligence community. Additionally, IAIP has yet to successfully complete the difficult task of comparing and prioritizing assets within and across sectors, but it plans to have an interim assessment done by the end of 2006. IAIP's challenge in the final three phases (evaluating alternatives, selecting approaches, and implementation and monitoring) are related heavily to IAIP's unique role: It recommends what the security priorities should be to other federal agencies and nonfederal stakeholders and recommends how best to address them, but it is largely dependent on other stakeholders, public or private, to take any actions. The decision to implement security improvements is made by stakeholders alone. Moreover, IAIP acknowledges that it can further leverage work that has already been done in this area by other federal agencies that have regulatory authorities over certain private sector infrastructure owners. IAIP's challenges center on developing credible guidelines and approaches that can leverage work already done and foster concurrence in risk analysis results and encourage actions to be taken.

Table 9: Summary of Progress Made and Challenges That Remain in IAIP's Risk Management Approach

Risk management phase	Examples of progress made	Examples of remaining challenges
Strategic goals, objectives, and constraints	Strategic goals have been laid out in various national strategies, and IAIP issued the Interim National Infrastructure Protection Plan (NIPP), which, among other things, is intended to guide the process for identifying, comparing, and prioritizing critical assets within and across sectors.	As IAIP works to complete the interim NIPP, it will be challenged to develop performance measures and detailed timelines or target dates for identifying and prioritizing critical infrastructure.
Risk assessment	IAIP has developed a national database of critical infrastructure assets and a series of benchmark threat scenarios to be used to analyze potential attacks. IAIP has used these scenarios to develop data collection instruments for two types of assets (nuclear plants and chemical plants) to assess their vulnerabilities.	IAIP faces challenges in developing a methodology so that it can develop data on the relative likelihood of various threat scenarios—a key element of risk assessment it must conduct under the Homeland Security Act. It also faces challenges in developing a methodology for prioritizing assets within and across sectors.
Alternatives evaluation	IAIP has developed tools for owners and operators of selected critical infrastructure assets to estimate the consequences of an attack and perform vulnerability assessments. This information is a prerequisite when valuing costs and benefits and prioritizing among different assets.	IAIP and the owners or operators of critical infrastructure may not agree on the costs and benefits of protective actions. Developing the methodology for prioritizing assets will also be important for progress in this phase. IAIP plans to develop procedures in 2006 for quantifying costs and benefits.
Management selection	IAIP is pursuing partnerships to encourage the responsible owners and operators to implement IAIP recommendations. IAIP is also developing a risk management decision support framework to facilitate government authorities' selection of risk management policy, programs, and budgetary options.	In most cases, IAIP does not have authority to make the selection; its role in this regard is advisory. Thus, its challenge is to develop ways to help ensure that owners, operators, and state and local government authorities make informed choices, ensure that federal decisions are informed by risk-based data, and leverage the regulatory authorities of other agencies.
Implementation and monitoring	IAIP has limited responsibilities in implementing programs that result in improved infrastructure protection. It provides funds to ODP through a Buffer Zone Protection Program that involves efforts to reduce vulnerabilities in and around facilities and assets.	IAIP is similarly challenged by a lack of authority in implementing protective measures to protect critical infrastructure. Also, IAIP cannot require state and local governments to use federal funds on specific infrastructure protection measures. In addition, IAIP is challenged to get intelligence data specific enough to develop measures for determining whether protective actions are actually deterring or minimizing the impact of terrorist attacks.

Source: GAO analysis of IAIP's risk management practices.

IAIP Plays a Key Role in Evaluating Risk across Infrastructure Sectors

While risk management is one of several tools for the Coast Guard and ODP, risk management is central to one of IAIP's key missions, which is to establish a risk management framework across the federal government to protect the nation's critical infrastructure and key resources.[1] The Homeland Security Act of 2002 made IAIP responsible for critical infrastructure protection (CIP) functions, charging IAIP with broad responsibility for developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States. IAIP's statutory responsibilities require it to conduct risk management activities on a national scale and to gather the information needed to do so from other federal agencies, state and local government agencies, and private sector entities.[2] By statute, IAIP is responsible for

- identifying, detecting, and understanding threats in light of actual and potential vulnerabilities to the homeland;
- conducting comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States;
- conducting risk assessments to determine the risks posed by particular types of terrorist attacks and how likely they are to succeed, as well as the feasibility and potential efficacy of various countermeasures;
- identifying priorities for protective and support measure by DHS, other federal agencies, state and local governments, the private sector, and other entities; and
- recommending measures to protect the critical infrastructure and key resources of the United States in coordination with other federal agencies and in cooperation with state and local governments, the private sector, and other entities.[3]

In December 2003, the President issued Homeland Security Presidential Directive-7, *Critical Infrastructure Identification, Prioritization, and Protection*, which established the framework in which IAIP carries out its responsibility of coordinating the overall national CIP effort. Current CIP

[1] The Homeland Security Act incorporates the definition of "critical infrastructure" used in the USA PATRIOT Act of 2001, meaning "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The Homeland Security Act defines "key resources" as "publicly or privately controlled resources essential to the minimal operations of the economy and government." 6 U.S.C. § 101.

[2] See generally 6 U.S.C. 121(d).

[3] Id. 121(d)(1), (2), (3), (6).

policy, as described in HSPD-7, defines responsibilities for DHS, sector-specific agencies, and other departments and agencies. It instructs federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent and deter attacks, and mitigate the effects of any attacks that may occur.

To ensure the coverage of critical sectors, HSPD-7 designated sector-specific agencies for the critical infrastructure sectors identified in the National Strategy for Homeland Security (see table 10). These agencies are responsible for infrastructure protection activities in their assigned sectors, which include coordinating and collaborating with relevant federal agencies, state and local governments, and the private sector to carry out their responsibilities and facilitating the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. For example, the transportation sector, for which the Department of Homeland Security is assigned responsibility, includes the movement of people and assets that are vital to the nation's economy, mobility, and security. The maritime shipping infrastructure, a component of the transportation sector, includes ports and their associated assets, ships, passenger transportation systems, and other maritime transportation assets. Each sector may also include a number of systems and "key assets"—some of which include individual targets whose attack could cause large-scale human casualties or property destruction, or profoundly damage national prestige and confidence.[4]

[4] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets identifies five key assets. The key assets and lead federal agencies are as follows: national monuments and icons (Department of the Interior); dams, locks, and levees (Department of Homeland Security); government facilities (Department of Homeland Security); commercial and community assets (Department of Homeland Security); and nuclear reactors, materials, and spent fuel (Department of Homeland Security, working with the Nuclear Regulatory Commission and, as appropriate, the Department of Energy). When we use the term "critical infrastructure" in this chapter, we are referring both to the 13 sectors and to the five key assets.

Table 10: Critical Infrastructure Sectors and Lead Federal Agencies

Sector	Sector-specific agency
Agriculture	Department of Agriculture and Department of Health and Human Services
Banking and finance	Department of the Treasury
Chemicals and hazardous materials	Department of Homeland Security (IAIP)
Defense industrial base	Department of Defense
Emergency services	Department of Homeland Security (IAIP)
Energy	Department of Energy
Food	Department of Agriculture and Department of Health and Human Services
Government	Department of Homeland Security (Federal Protective Service)
Information technology and telecommunications	Department of Homeland Security (IAIP)
Postal and shipping	Department of Homeland Security (TSA)
Public health and health care	Department of Health and Human Services
Transportation	Department of Homeland Security (TSA)
Drinking water and water treatment systems	Environmental Protection Agency

Source: GAO analysis of the President's national strategy documents and HSPD-7.

Under HSPD-7, the overall national CIP effort is to be coordinated by DHS, a responsibility carried out by IAIP, subject to the DHS Secretary's direction and control, as provided in the Homeland Security Act of 2002. The DHS Secretary has several overarching CIP responsibilities under HSPD-7, including identifying, prioritizing, and coordinating CIP within and across sectors, with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties. In addition, the Secretary is required to establish uniform policies, approaches, guidelines, and methodologies for integrating CIP and risk management activities within and across sectors, along with metrics and criteria for related programs and activities.

Strategic Goals, Objectives, and Constraints: High-Level Goals in Place and Interim Plan Drafted, but Performance Measures and Milestones Have Yet to Be Developed

A number of strategic goals are in place to guide IAIP's broad responsibilities. They stem from the Homeland Security Act of 2002 and the following executive branch documents:

- *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.*[5] Issued in February 2003, this strategy identified a set of national goals and objectives and outlined the guiding principles that underpin efforts to secure the critical infrastructure and key resources of the United States. The strategy recognizes that adequate protection of critical infrastructure requires (1) comprehensive threat assessment and analysis; (2) effective and efficient risk assessment; and (3) security baselines, standards, and guidelines.

- *Homeland Security Presidential Directives 7 and 8.* Both directives were issued on December 17, 2003. HSPD-7 established a national policy for federal departments and agencies to enhance the protection of critical infrastructure and key resources and made DHS responsible for establishing uniform policies, approaches, guidelines, and methodologies for integrating nationwide infrastructure protection and risk management activities. HSPD-8 calls for a national preparedness goal that balances the potential threat and magnitude of terrorist attacks with the resources required to prevent, respond to, and recover from them—a risk management approach calling for an estimate of the likelihoods and expected consequence of possible terrorist attacks that takes finite resources into account.

- *The Interim National Infrastructure Protection Plan (interim NIPP).* The Secretary of DHS assigned IAIP the responsibility for developing a national infrastructure protection plan. The interim NIPP was released in February 2005.[6] It calls for the use of a risk management framework that takes into account threats, vulnerabilities, and consequences when comparing and prioritizing critical infrastructure and deciding what

[5] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets is complemented by the National Strategy to Secure Cyberspace. Also issued in February 2003, the National Strategy to Secure Cyberspace provides direction to the federal government departments and agencies that have roles in cyberspace security and identifies steps that state and local governments, private companies and organizations, and individuals can take to improve collective cybersecurity.

[6] In November 2005, DHS issued a Draft National Infrastructure Protection Plan for comment. We did not evaluate the draft plan because our field work had already been completed.

actions to take to protect them. This framework is intended to be carried out both within sectors and nationally across sectors. It is to contain steps for narrowing the overall set of assets to those that are most critical at a national level.

We have reported that the interim NIPP is not a comprehensive document, and IAIP faces several challenges in making it more comprehensive.[7] These challenges are in two main areas:

- *Performance measures*. Although the interim NIPP did not contain performance metrics to measure effectiveness, it recognized that they are needed and calls on IAIP and the sector-specific agencies to develop them. According to IAIP officials, this is being done in two phases. For the first phase, IAIP has identified a set of basic core metrics that can be used to evaluate performance across all sectors, as called for in the interim NIPP. IAIP is also working with agencies responsible for specific sectors to develop a supplemental set of metrics for each sector. The intent of this measurement process is to provide DHS and the sector-specific agencies with feedback on where and how they should focus their resources to be most effective. According to IAIP officials, the second phase involves, in part, monitoring the progress of each sector in implementing the risk management framework laid out in the interim NIPP. To date, however, IAIP and the sector-specific agencies have not completed the performance metrics called for in the interim NIPP.

- *Milestones and timelines*. The interim NIPP did not contain milestones for the development of sector-specific plans or timelines of target dates for identifying and prioritizing critical infrastructure. According to IAIP officials, the final version of the NIPP, after undergoing interagency review, will be released in 2006, and it will contain milestones and timelines for the initial phase of developing performance metrics. It is not clear, however, if this final version will contain milestones and timelines for sector-specific plans or for completing the process of prioritizing critical infrastructure.

[7] GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*, GAO-05-827T (Washington, D.C.: July 19, 2005).

Risk Assessment: IAIP Faces Substantial Gaps and Has Made Limited Progress

IAIP's progress in risk assessment has not been as extensive as the Coast Guard's or ODP's. Its area of greatest progress is in developing a national database of assets that constitutes the nation's critical infrastructure. In two other key respects, however, it faces major challenges in carrying out requirements specified in law or policy directives. These challenges are in developing adequate data on threats and creating a methodology for making cross-sector comparisons.

Progress Is Greatest on Database of Critical Assets

IAIP has developed the National Assets Database (NADB), an inventory of approximately 80,000 assets, as a starting point in being able to evaluate and prioritize them. The NADB includes such facilities as nuclear power plants, pipelines, bridges, stadiums, and locations such as Times Square. Assets in the NADB are gathered from a variety of public and private sector sources, including federal, state, and local databases; prior studies containing lists of infrastructure and resources; and sector-specific data collection activities. The database is revised as assets are added and removed in collaboration with state and local officials and with representatives of sector-specific agencies. According to IAIP officials, this database is intended to produce baseline data that will later allow for assessments of vulnerabilities by location, within sectors, and across sectors.[8]

Development of Threat Data Faces Challenges

IAIP has begun work to develop threat scenarios and analyze them. The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), staffed by sector specialists and intelligence analysts with backgrounds from the intelligence community, is responsible for generating these plausible threat scenarios—called benchmark threats. HITRAC has developed 16 benchmark threats, such as a suicide bomber, a vehicle-borne improvised explosive device, and a weapon of mass destruction. IAIP faces two substantial challenges, however, in completing this work.

- *Relative probability for threat scenarios not yet developed.* First, IAIP faces challenges in developing a way to differentiate the relative probability of various threats. Under the Homeland Security Act of

[8] GAO did not analyze the data in the database and cannot comment on the database's reliability. The Congressional Research Service has raised a number of issues concerning the data integrity of the IAIP asset database. See Congressional Research Service, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences* (Washington, D.C.: February 2005).

2002, IAIP must perform risk assessments to determine the risks posed by particular types of terrorist attacks, including an assessment of the probability of success of such attacks.[9] IAIP officials stated that a lack of intelligence data and law enforcement data limits their ability to develop the relative probability for various threat scenarios, and for this reason, they have focused their initial efforts on developing vulnerability and consequence data. According to IAIP officials, the intelligence community—including the intelligence components of DHS—has been unable to provide detailed intelligence on threats to most sectors, infrastructure, assets, or asset types.[10] Assigning equal likelihood to various threat scenarios would mean IAIP's risk assessments will not include key threat data on the capabilities and intent of terrorist groups, the history of terrorist threats on various asset types, or the existence of terrorist cells domestically or internationally. And because data on the relative likelihood of threat scenarios are not included, the assessments will emphasize high-consequence events that may have a low probability of occurring. This approach is bound to result in potentially unreliable or incomplete data on where to establish priorities. In September 2005, IAIP officials told us that they recognize the importance of developing data on the relative likelihood of an attack type, and that doing so is part of their responsibility for meeting the requirements of the Homeland Security Act. Officials told us that they plan to assess the likelihood of threats by having HITRAC develop consistent comparative threat assessments by integrating intelligence sources, law enforcement data, and suspicious activity reporting with subject matter expertise. IAIP officials caution, however, that the directorate may not be able to estimate the relative likelihood of some threat scenarios, and as a result, some assessments may emphasize high-consequence events that have a low probability of occurring. Also, officials indicated that some inaccuracy is to be expected when HITRAC examines the intent and capability of an adversary whose plans are concealed and that it will be

[9] See 6 U.S.C.121(d)(2). IAIP considers the combination of the threat (relative likelihood of the attack type) and vulnerability (likelihood of the adversary's success) to represent the relative likelihood of a successful attack occurring.

[10] While the intelligence community does rank threats, IAIP does not find such information useful in developing data on threats. Intelligence components of DHS and other intelligence agencies routinely generate strategic threat assessment matrices and reports detailing the most likely targets and modes of terrorist attack. These assessments break down infrastructure and assets into categories and rank them, numerically or otherwise, according to the relative likelihood of attack within and across categories. However, IAIP officials said that the information was not specific to individual assets.

important to reduce the potential of low-confidence assessments having undue influence when long-term investment decisions are made.

- *Vulnerability assessments not yet developed for many infrastructure sectors*. Second, IAIP has not yet developed vulnerability assessments for the full spectrum of infrastructure sectors. As of August 2005, IAIP had managed the development of vulnerability assessment questionnaires for two components of critical infrastructure—nuclear facilities and chemical facilities. Initially, IAIP's contractor was scheduled to assess asset types in 8 of the 18 sectors and key assets by the end of 2005. However, according to IAIP officials this work will be done by the end of 2006.[11] IAIP officials did not have an estimate as to when the assessments would be complete for all other sectors of critical infrastructure that it is responsible for assessing.[12]

Methodology for Cross-Sector Comparisons Has Experienced Setbacks

IAIP has experienced setbacks in its attempts to meet HSPD-7's requirement to develop a strategy for identifying, prioritizing, and coordinating the protection of critical infrastructure. To prioritize the protection of this infrastructure, IAIP has been working for about 2 years on a methodology for assessing vulnerabilities of critical infrastructure to help inform comparisons of risks on an intrasector and cross-sector basis. This methodology has been delayed because of methodological concerns, and IAIP's schedule for completing various other activities needed to meet the requirement is dependent on the methodology and now appears uncertain.

IAIP developed an analytical assessment tool known as the Risk Analysis and Management for Critical Assets Protection methodology (RAMCAP).

[11] After grouping all components of critical infrastructure by sector, IAIP plans to ask the owners or operators to complete a questionnaire—called a "top screen"—that provides an assessment of consequential losses arising from a worst-case scenario that assumes total loss of the asset. Once this information is gathered and assessed, assets considered to be of sufficient consequence are evaluated on vulnerability, using three elements: potential method of attack, probability of success, and consequences of the attack (including secondary and tertiary effects). By applying this information to the selected subset of assets, IAIP seeks to identify the assets of greatest vulnerability and identify strategies that hold the greatest potential benefits. Much like the consequence assessment, the vulnerability assessment is carried out by eliciting the opinions of experts, usually the owner/operator, for a specific piece of infrastructure.

[12] IAIP has plans to address the risks involved in protecting additional critical infrastructures, such as stadiums, though a tool called the Vulnerability, Identification, and Self-Assessment Tool. This tool will allow owners and operators to assess vulnerabilities in and around their facilities.

RAMCAP was begun in November 2003, when DHS awarded the American Society of Mechanical Engineers (ASME) a $1.6-million grant to develop an overarching methodological guide for the private sector to assess its terrorism security risks. Originally, DHS expected RAMCAP to advance homeland security efforts by providing a usable, affordable vulnerability and risk assessment methodology for owners and operators to use that would inform risk management decision in the private sector. Now, IAIP views it as an independent effort that will complement IAIP risk assessment efforts at comparing risks within and across sectors.

When RAMCAP was released for comment in April 2004, ASME received comments from over 100 officials from industry, academia, and government. A peer review process produced additional comments. The comments centered on several issues, including concern about the amount of resources needed to assess risks and the limited benefits in creating self-assessments for industry without knowing what the purpose of the effort involved.[13] In June 2004, ASME altered its approach based on this feedback and began a broad outreach effort to involve industry in developing vulnerability assessment modules.

In December 2004, IAIP awarded a $4 million contract to ASME to continue its efforts in developing RAMCAP and vulnerability assessment modules for owners and operators of asset types in eight sectors.[14] After developing pilot modules for the chemical and nuclear industries, in August 2005, ASME produced a new working draft of RAMCAP. According to IAIP, RAMCAP may undergo minor revisions as more modules are completed. IAIP officials stated that more substantial revisions to RAMCAP will likely occur when IAIP broadens its approach to infrastructure protection by examining the entire systems and interdependencies within and across sectors.

In September 2005, IAIP informed us that it is developing a National Comparative Risk Assessment for the 18 critical infrastructure sectors and

[13] IAIP and the private sector agreed that the goal of the self-assessments was to satisfy the information needs of DHS.

[14] The eight categories of assets are commercial nuclear power plants, commercial spent nuclear fuel facilities, chemical plants, petroleum refineries, liquefied natural gas storage facilities, subway systems (including bridges and tunnels), railroad systems (including bridges and tunnels), and highway systems (including bridges and tunnels). The vulnerability assessments for the chemical sector and nuclear power plants were pilot projects.

key assets, and it plans to complete an interim assessment by the end of 2006. The assessment has several phases. It involves sector-specific agencies identifying the top 100 high-risk systems and assets in their sector based on potential consequences. IAIP officials said it requested agencies to develop their lists by July 2005. However, the degree to which agencies will be able to fully respond to the request is uncertain. For example, as of July 2005, the Transportation Security Agency had begun but not yet completed a risk assessment for the passenger rail sector, and it did not indicate when the assessment would be done. Additionally, TSA did not expect to have the first version of its sector-specific plan—the plan that describes its risk assessment methodology—until February 2006. Until agencies such as TSA complete their assessments and develop their sector-specific plans, they will not be able to determine relative risks within their sector in a consistent fashion.[15]

Whether IAIP will be able to complete this interim assessment by the end of 2006 may be complicated by two other factors. First, in September 2005, IAIP officials said that IAIP still needs to award the contract for this effort, and officials did not provide a schedule for when this would occur. Second, the degree and extent to which IAIP will need to obtain input from the private sector in developing this assessment tool is unclear. In developing the vulnerability assessment modules for sector-specific industries, IAIP's consultant and industry groups worked extensively with each other in developing the modules. If similar coordination and communication efforts are needed to complete the interim assessment, it may call for additional time and resources.

According to IAIP officials, once the initial rankings are made, subject matter experts will review the results and the results of previous analyses will be used to refine the rankings within a sector and ultimately across sectors. IAIP plans to use the interim results to inform homeland security grant programs and serve as a basis for further risk management efforts. The results of the vulnerability assessment modules that are being developed will inform the national assessment and will act as a basis for interaction with the private sector, according to IAIP.

The interim National Comparative Risk Assessment is intended to meet the immediate need of examining relative risk within and across sectors.

[15] GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-05-851 (Washington D.C.: Sept. 9, 2005).

However, there are limitations on the degree to which the interim assessment will produce comparable, consistent, and reliable data for setting national priorities. First, only vulnerability assessments of asset types in 8 of 18 sectors and key assets are scheduled for completion by the end of 2006, while the schedule for completing assessments on other sectors or asset types is unclear—suggesting that vulnerability data on some sectors will be more reliable than data on other sectors. Second, the interim assessment will likely involve a heavy emphasis on consequence-related data, and less information on the relative likelihood of threat scenarios and data on vulnerability—two major components of risk assessment. Third, as sector-specific agencies develop their list of high-risk assets, it is unclear whether they will do so in a consistent and uniform fashion, because the overarching framework that guides these actions is not yet in place. In September 2005, we reported that completing the element of the framework that defines concepts, terminology, and metrics for assessing risk limits DHS's ability to compare risk across sectors.[16] IAIP recognizes that engaging sector-specific agencies in assessing risk in a consistent way is key. IAIP now intends the National Comparative Risk Assessment to provide such guidance, but until this assessment is issued, it is unclear where the guidance will come from. Limitations such as these, according to IAIP, are driven to some degree by resource and time constraints.

Evaluating Alternatives: Lack of Guidance and Consensus on Costs and Benefits Creates Challenges

The alternatives evaluated by IAIP differ somewhat from the alternatives evaluated by the Coast Guard (as discussed in chapter 2) or ODP (as discussed in chapter 3). The Coast Guard evaluates alternatives related directly to how it deploys its own resources, such as increasing security patrols, boarding suspicious vessels, creating and enforcing security zones, and using its regulatory powers to force maritime facilities to adopt protective measures. ODP evaluates alternatives that relate directly to its grant awards; the alternatives are the various funding proposals for security-related infrastructure improvements. In contrast, the alternatives that IAIP evaluates are generally not based on actions IAIP can take. Instead, they are based on identifying, from a national standpoint, the (1) areas of greatest risk and (2) infrastructure protection strategies that offer the greatest benefit for the cost involved. In this regard, IAIP faces several challenges.

[16] GAO-05-851.

One challenge faced by IAIP in evaluating alternatives is the difficulty in valuing costs and benefits in a homeland security setting—an important tool for evaluating alternatives. OMB has guidance for federal agencies on how to evaluate alternative government actions, but this guidance is of limited use in assessing alternatives for risk management for homeland security programs. OMB has identified various tools it considers useful in planning, such as cost-benefit analysis, capital budgeting, and regulatory decision making.[17] However, such tools are difficult to apply to homeland security expenditures, even when such application is encouraged in the National Strategy for Homeland Security, because the benefits of homeland security investments are hard to quantify. Because OMB guidance is relatively silent on acceptable treatment of nonquantifiable benefits, there is a lack of criteria to guide federal analysts in conducting risk management. In response to our inquiries, OMB officials told us that they have not been involved in implementing Homeland Security Presidential Directive-7, which is related to critical infrastructure protection. In addition, they said that they have not been developing, nor did they have plans to start developing, guidance on risk management methodologies for federal agencies to use for homeland security programs. They said that they would rely on DHS and IAIP to take the federal government lead in developing such methodologies. IAIP officials said they plan to develop procedures in fiscal year 2006 for quantifying costs and benefits of mitigation strategies.

Another challenge faced by IAIP in evaluating alternatives, at least in terms of ranking assets and protective actions to prevent and mitigate attacks, is that other entities responsible for taking such protective actions may use different criteria for evaluation. That is, the federal, state, local, or private sector entities that own and operate much of the nation's critical infrastructure may disagree with IAIP on how to evaluate alternatives through assessing benefits and costs or other types of evaluation. This lack of consensus could lead to two separate evaluations of alternatives—one by IAIP and one by the entity that owns and operates the asset. While IAIP may view certain assets or protective actions as critical, those responsible for the assets and protective actions may view the assets and actions as marginal or not necessary at all, or vice versa. According to IAIP officials, state and local government and industry stakeholders will benefit from using the same assessments, but the value that is placed on the assessment may differ from one stakeholder to another. As an example, Washington

[17] OMB Circulars A-11 and A-94.

state emergency management officials told us that their initial listing and ranking of critical assets was much different than that developed by IAIP. State officials may place greater weight on attack scenarios that result in impacts on children or disadvantaged communities. Industry may place greater weight on scenarios that disrupt the long-term viability of a business. IAIP's challenge is discerning whether federal risk concerns are managed appropriately and that the costs for managing risks are assigned as much as possible to the authority that benefits from the activity. In addition to these considerations, Congress also has a role in appropriating federal funding of protective programs.

Management Selection: IAIP Challenged in Protecting Infrastructure because of Its Limited Role in Selecting Alternative Protective Measures

As with the alternatives evaluation part of GAO's framework, IAIP's management selection differs from how the Coast Guard or ODP makes decisions. While the Coast Guard decides what protective measures to take and ODP decides which applicants receive funding for port security, IAIP is not in a position to direct others on how to act. IAIP officials said that while they have the responsibility of helping set risk-based priorities concerning where resources should be spent for protecting critical infrastructure, IAIP does not have the authority to direct the management of these resources in many cases. For example, IAIP does not have authority to compel owners and operators of critical infrastructure to take action. Instead, IAIP recommends the relative priority of critical infrastructure and specific protective measures. Other entities, such as owners, operators, or agencies with more direct regulatory responsibilities, can then act on IAIP recommendations and technical advice. The one exception is IAIP's Buffer Zone Protection Program, which we discuss in the section following on implementation and monitoring.

At the departmental level, DHS may use the IAIP priority list to direct one of its component agencies to take specific actions. As examples, IAIP priorities could be used by U.S. Customs and Border Protection to increase the scrutiny of cargo containers at a specific port terminal, by the Secret Service to increase security for the President, by the Federal Emergency Management Agency to help improve local response capabilities near specific facilities, or by ODP to provide grants to specific facilities. In some cases, DHS components may have some authority over private infrastructure owners—such as the Coast Guard's regulatory powers related to implementing the Maritime Transportation Security Act. For example, the Coast Guard approves vulnerability assessments and mitigation strategies developed by owners and operators of facilities and vessels and it reviews whether the owners and operators are complying with their plans. However, in most cases, DHS and its components do not have authority over the owners and operators of critical infrastructure, particularly in the private sector.

Thus, the challenge for IAIP (and DHS at the department level) is that it generally does not have authority over the entities that make management decisions to select among alternative protective measures. In such cases, IAIP's role is limited to providing information on how it views the relative strengths and weaknesses of the alternatives and, sometimes, technical advice on how these entities could improve the security of their assets. IAIP officials said they use their expertise and powers of persuasion to get the owners and operators to take specific protective actions. IAIP officials also said that IAIP works closely with industry groups to set standards and promote voluntary compliance.

Certain protective measures could have application across multiple threat scenarios. The interim NIPP does not describe what IAIP's plans are for analyzing its benchmark threat scenarios and developing information that could help owners and operators reduce risk by protecting their facilities with countermeasures that address multiple scenarios. For example, improving security operations could reduce the risk of multiple threats, such as suicide bombers, truck bombs, or weapons of mass destruction. Having sufficient emergency supplies could address the consequences of casualties or damaged infrastructure that occur from various attack modes. By not having plans to develop information on what countermeasures could address multiple threat scenarios, IAIP is limited in it ability to provide information that informs owners and operators of facilities of ways to protect their facilities in a cost-effective fashion. According to IAIP, it is considering this in the cost-benefit framework that is being developed.

IAIP's lack of authority over the owners and operators of critical infrastructure highlights the importance of coordination among different federal agencies. Several federal agencies with lead responsibilities for specific sectors of infrastructure do have regulatory authorities that could be used to set security standards and compel protective measures. For example, the Department of the Treasury and the Securities and Exchange Commission and other agencies have regulatory authorities over financial markets and can compel them to take certain protective measures. While DHS generally does not have authority over many of the assets in those sectors in which it has lead responsibility, some other federal agencies do. For example, the Nuclear Regulatory Commission, which issues licenses to commercial nuclear power plants, has clear regulatory authority over security matters at these facilities. While each sector has a Government Coordinating Council that includes representatives from federal agencies involved in the sector, IAIP recognizes that it can further leverage work that has already been done by other agencies that have regulatory authority over certain private sector owners. This condition brings attention to the need for IAIP to coordinate with these agencies to leverage federal authority in areas where oversight already exists.

Implementation and Monitoring: IAIP Is Also Challenged by Its Limited Role in Implementation and Limited Information on Effectiveness

IAIP has a limited role in implementing its own protective programs, as well as in monitoring the effectiveness and level of implementation of security risk management programs broadly. An example of IAIP's role in implementing protective programs is the Buffer Zone Protection Program. Managed by the Protective Security Division within IAIP, the program is designed to make it more difficult for terrorists to conduct planning activities or successfully launch attacks from the immediate vicinity of critical infrastructure and key resource targets. The goal of the program is to assist state and local government, local law enforcement, and owners and operators in preventing, defending against, preparing for, and mitigating the impacts of terrorist attacks. The program does so by making grants available, through ODP, to state and local law enforcement to implement buffer zone protection plans "outside the fence" of private facilities, as well as by conducting workshops and technical assistance visits.

However, IAIP's role in implementing protective measures is much more limited "inside the fence" because IAIP does not own or operate any assets, have regulatory authority over those entities that own or operate the assets, or provide funds for such entities. Owners and operators of the infrastructure assets—be they federal, state, local, or private—are responsible for implementing the protective actions needed. As previous GAO work has shown, public policy tools have been used as an approach to encourage increased private sector critical infrastructure protection efforts even when regulatory authority is lacking.[18] In terms of monitoring implementation of actions to increase the protection of critical infrastructure, however, IAIP does have a role. Its mission is to assess the overall state of critical infrastructure protection in the nation.

[18] GAO, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington D.C.: Feb. 28, 2003); and *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-715T (Washington D.C.: May 8, 2003).

In its monitoring role, IAIP faces a number of challenges. The first challenge is that there are currently no performance measures to evaluate the effectiveness of infrastructure protection. The interim NIPP, while calling for such measures, does not offer any. According to IAIP officials, such performance metrics will not be available before 2006. One of the difficulties encountered is that it is hard to develop performance measures to gauge homeland security activities that are directed at modifying terrorist behavior. For example, it is difficult to determine whether measures to improve the protection of critical infrastructure have a deterrent effect on terrorists. In some cases, deterring terrorists from attacking "hard" targets (those that are heavily protected) might have the effect of directing the terrorist toward attacking "soft" targets (those that are lightly protected).

Conclusions

IAIP's role in risk management is critical because of its breadth. IAIP has overall responsibility to identify critical assets across all sectors of the nation's infrastructure, as well as to play a lead role in developing methodologies and guidance for analyzing risks and assessing the benefits and costs of security alternatives. Progress in most areas of responsibility has been limited, and much challenging work remains to be done. In particular:

- Good threat data are critical to conducting risk management. During the course of our review, IAIP recognized the importance of developing information on the relative probability to various threat scenarios. Until better data on threats are developed, risk-based data may not fully inform decisions on where to establish priorities.

- Even with better threat data, assets cannot be compared across sectors without a methodology for doing so. Currently, IAIP is developing a methodology to do this, but it is not yet comprehensive, nor has it been applied. Until such a methodology is fully developed, IAIP will be challenged in conducting a national-level assessment of risks, a key element of IAIP's core responsibility. Without a methodology, it will not be possible for IAIP to make a determination of relative risks that could help inform decisions on resource allocation.

- Comprehensive planning and performance measures are necessary to clarify what needs to be done and to determine progress in critical infrastructure protection. The National Infrastructure Protection Plan is still in interim form, leaving open many questions about how specific sectors will be protected and how performance will be measured.

Without target dates for completing sector-specific plans and performance measures, it will not be possible to determine IAIP's progress in these areas. Additionally, without having plans to develop information on what protective measures could address multiple threat scenarios, IAIP's ability to inform owners and operators of ways to protect their facilities in a cost-effective fashion is limited.

In all, the lack of progress leaves many decision makers basically on their own to develop a way to determine where scarce resources need to be applied against almost unlimited numbers of assets to maximize the protection of critical infrastructure and security for the homeland.

Recommendations for Executive Action

To help ensure the development of risk management approaches to homeland security activities, we recommend that the Secretary of Homeland Security direct the Undersecretary for IAIP to undertake the following three actions:

- Work with the intelligence community to develop ways to better assess terrorist threats and use available information and expert judgment to develop a relative probability for various terrorist scenarios and provide this information to sector-specific agencies;
- As tasked by presidential directive, develop a methodology for comparing and prioritizing risks of assets within and across infrastructure sectors by including data on the relative probability of various threat scenarios;
- In completing the National Infrastructure Protection Plan, include target dates for completing sector-specific plans, developing performance measures, and identifying protective measures that could address multiple threat scenarios.

Agency Comments and Our Evaluation

In commenting on a draft of chapter 4, DHS, including IAIP, said that IAIP is taking steps to address recommendations in the report. In regard to our recommendation on working with the intelligence community to develop better threat data, DHS said it is working with the Coast Guard on a pilot project to do so. The pilot effort will be evaluated, improved upon, and then more broadly applied with stakeholders in the intelligence community pending their acceptance, according to DHS. In regard to our recommendation on developing a methodology for comparing and prioritizing risks within and across sectors, DHS responded that for fiscal year 2006 grants, a risk analysis methodology was applied that considers a small set of assets across sectors. With respect to our recommendation on completing the National Infrastructure Protection Plan, DHS stated that a draft plan is out for comment and that the issue of identifying protective measures that could address multiple threat scenarios is being addressed by IAIP. DHS also submitted technical comments under separate cover and we made changes where appropriate. Written comments from DHS are in appendix II.

Chapter 5: Overall Observations and Recommendations

Taken together, what do the efforts and experiences of these three components suggest about where DHS is with regard to managing homeland security efforts on the basis of risk? In our view, there are two key overall observations related to the degree of progress made, and two more related to next steps that need to take place. With regard to progress made, the first observation is that while considerable effort has been applied, much more remains to be done than has been accomplished so far. Across all three components, the most progress has generally been made on fundamental steps, such as conducting risk assessments of individual assets, and the least amount of progress has generally been made on developing ways to translate this information into comparisons and priorities across ports or across infrastructure sectors. Second, and closely related, progress among the three components' efforts has varied not only with the length of time the component has been at the job, but also with the complexity of its risk management task. With regard to next steps that would appear to add most value to making further progress, one key observation is that in the short term, progress is heavily dependent on continuing to make steady progress at improving basic policies, procedures, and methods for risk assessments and other phases of the risk management framework outlined in chapters 2, 3, and 4. Each component has an admittedly difficult set of challenges ahead, but progress has to be built on taking these incremental steps and doing them well. The final observation is related to a critical longer-term need: more guidance, direction, and coordination from DHS. The challenges and difficulties associated with creating a coordinated, coherent risk management approach to the nation's homeland security have been widely acknowledged since the events of September 11 and the creation of DHS. One of the presidential directives calls on DHS to provide such guidance, but the agency has yet to do so. As individual components begin to mature in their risk management efforts, the need for consistency and coherence becomes even greater. Without it, the prospects increase for efforts to fragment, clash, and work at cross purposes.

First Observation: Much Remains to Be Done

There is a long way to go in implementing risk management successfully in port security—and an even longer way to go in implementing risk management in homeland security in general. One main reason is the sheer amount of work that must be done. Five years ago, before the September 11 attacks, the various terrorist scenarios seemed more remote and less certain than the hard reality brought on that day. September 11 changed this perspective dramatically. The work involved is immense and cuts across many jurisdictional boundaries. Federal agencies are called on to strengthen their partnerships with one another and to work more closely with thousands of state, local, and industry stakeholders.

A second major reason is that applying risk management to terrorism has no well-established precedent. Parts of the private and public sectors have used risk management principles for decades. However, doing so in a homeland security setting is a highly difficult task that remains in its embryonic phases. The components we reviewed face daunting challenges in weaving a concern for risk into the annual cycle of management review and budget decisions. Across the federal government, this challenge is magnified and complicated because of the number of agencies charged with carrying out risk management. This is an extraordinarily difficult effort with no clear road map of ways to strategically integrate a concern for risk into management decisions.

The fact that so much work remains is not the result of inaction by federal agencies. In the agencies and programs we examined, activities were often extensive and wide-ranging. Some activities, such as IAIP's attempts to develop risk assessment criteria for its comparisons across risk sectors, have had limited success, compounding the problem. The underlying point, however, is that this is an extraordinarily difficult effort with no clear and direct precedent to act as a guide. Implementing risk management in port and homeland security will take time and care, and this challenge will require ingenuity in adopting risk management techniques to this new application in a cost-effective way.

The progress that has occurred to date in the agencies and programs we examined has been primarily in the activity that most people would perhaps associate most readily with risk management—conducting assessments to determine what the risks are at specific ports and facilities. While much remains to be done even there, progress has generally been slower on ways to approach risk management strategically—that is, with a clear set of measurable objectives, a clear knowledge of the options available for addressing risks and the trade-offs involved with these options, and evaluation and feedback mechanisms for continuing to refine and strengthen the approach.

Observation Two: Progress Varies by Component and Reflects Key Characteristics of the Component and the Scope of Its Risk Management Efforts

The three components we studied have made varying degrees of progress in risk management, and to a degree their progress is related to three main factors: how long they have been at the task, how organizationally stable they are, and the scope of what they are trying to do. The Coast Guard, for example, is furthest along among the three components, reflecting in part where it stands in relationship to all three of these factors. It has been at the task the longest of the three components, having begun work on implementing risk management in its port security efforts immediately after the September 11 attacks. Its primary risk assessment tool at the port level, PS-RAT, was implemented in November 2001, and by August 2002, prior to the creation of DHS and the port security framework called for under the Maritime Transportation Security Act of 2002, it had begun security assessments at major U.S. ports. To a degree, these early efforts were learning experiences that required changes, but the Coast Guard was able to build on its early start. The Coast Guard also had the greatest organizational stability of the three components. It moved into DHS as an already established entity with an organizational culture spanning decades, and its organization and mission were not significantly altered by moving into DHS. Finally, with regard to the scope of its risk management activities, the Coast Guard's work is specific to port locations, where it has direct and primary responsibility for carrying out security responsibilities. With its focus on ports, the Coast Guard does not have to address a number of the critical infrastructure sectors laid out in national preparedness policy, such as banking and finance, information and technology, and public health. Even so, the Coast Guard's experience to date shows that as the scope of activity widens, even within a single sector, complexities develop. For example, the Coast Guard has prioritized risks within individual ports, and it has actions under way to assess risks across ports, but using this information to strategically inform the annual program review and budget process will require further attention.

ODP has made somewhat less progress than the Coast Guard. Relative to the Coast Guard's progress, its progress reflects a later start, an organization with much less institutional maturity, and a different role from the Coast Guard's in that ODP provides grant money rather than directly setting security policy. ODP was transferred from the Department of Justice to the Department of Homeland Security in 2003. While ODP's early grant approval efforts had some risk management features in place, its main strides in risk management have come in the procedures recently adopted for the fiscal year 2005 grants. In moving toward risk management, ODP has found ways to allow information from the Coast Guard and IAIP to inform its decision making. This is an encouraging and important sign, because the success of risk management efforts depends in part on the ability of agencies with security responsibilities to share and use each others' data and expertise. Although both the Coast Guard and the port security grant program administered by ODP have port security as their focus, ODP's more limited scope of responsibility has also had an effect on its risk management efforts. First, because ODP's role is to award grants that support federal priorities in port security, its progress in risk management depends to a degree on the progress made by federal agencies in determining what their own port security performance measures should be. Second, ODP's funding priorities are subject to criteria other than risk, as the fiscal year 2004 grant awards demonstrate. That year, after creating an initial list of awardees based in part on risk, and without regard to ability to pay, ODP extensively revised the list and awarded grants to entities considered to have fewer funding alternatives.

Of the three components, IAIP is the least far along in its risk management efforts. All three factors have had an effect on this progress: IAIP has been at its task for a relatively short time; it is a new component; and relative to the Coast Guard and ODP, the scope of its efforts is much broader and more difficult. IAIP was created under the Homeland Security Act of 2002, giving the directorate little time to acquire institutional maturity. In addition to taking on difficult tasks like risk management, IAIP faces other institutional challenges, such as establishing new management systems, developing sound human capital practices, and integrating its efforts with those of the rest of DHS. Further, the scope of its risk management activities extends well beyond the port-focused activities of the Coast Guard or ODP. IAIP is responsible for conducting risk assessments for every critical infrastructure segment in the nation. As demonstrated by the experience of its RAMCAP methodology for comparing risk across sectors, IAIP remains challenged in meeting that responsibility. Its lack of progress reflects the same lesson that emerges from the Coast Guard's experience in trying to expand the focus of risk assessments beyond a single port: The complexity of risk management appears to grow exponentially as the focus expands beyond a single location or single type of infrastructure. This complexity may help explain IAIP's lack of progress, but IAIP is unable at this time to provide adequate assurance to Congress or the country that the federal government is in a position to effectively manage risk in national security efforts. Steps have been small; by far the biggest work is yet to come.

Observation Three: In the Short Term, Further Progress Is Still Heavily Dependent on Completing and Improving Basic Policies, Procedures, and Methods

Acknowledging that the nation still has far to go in establishing a sound risk management approach to security should not obscure the need to continue taking small, but critical, steps—building on incremental advances. The three components we reviewed have actions under way to improve their risk management approach, and their experience indicates that much of the immediate work should remain focused on basic steps needed to implement all components of the full risk management framework. The recommendations we make in chapters 2, 3, and 4 include component-specific steps for what needs to be done. In overview, these specific recommendations cluster around several major themes related to the five phases:

- *Setting strategic goals, objectives, and constraints*: While all three components have broad-scale goals in place, none has yet tied these goals to specific and measurable results. Without such measures, it is difficult to gauge what progress has been made in improving security and what security gaps remain. The Coast Guard is furthest along: It has tied its goals to activity levels, such as the number of patrols conducted or vessels inspected, and it is working toward developing outcome-based measures. This is a good step, but without such measures in place, it is not possible to see how programs reduce risks, improve security, or identify gaps in security that remain. All three components would benefit from specifying in clear and measurable terms what their efforts are designed to accomplish.

- *Conducting risk assessments*: All three components can improve their risk assessment techniques. All three were challenged by a general lack of detailed information on capabilities and intentions of terrorist groups as this relates to various threat scenarios. They took different approaches in response: The Coast Guard, for example, used threat scenarios as substitutes for detailed threat information and is working on assigning likelihood to each in order to determine where risks might be greatest, while IAIP evaluated the consequences of certain possible attacks and focused its analysis of vulnerabilities on the attacks with the greatest consequences. Approaches that do not include information on the likelihood of various threat scenarios have limitations that affect the degree to which agencies are able to determine how to best focus their efforts on areas of greatest risk. Efforts to strengthen both data, methodology, and policy would increase the reliability of their results.

- *Evaluating alternatives*: All three components face problems in measuring the costs and benefits of different measures for preventing or mitigating terrorist attacks. These include developing ways to measure costs incurred by a broad range of public and private stakeholders and developing ways to measure benefits (such as deterrence) when these benefits may not be quantifiable. These difficulties are particularly great for IAIP, which must be able to measure costs and benefits associated with mitigation strategies that reduce vulnerabilities at critical infrastructure in all sectors. These difficulties are compounded by the complexity in valuing costs and benefits in the area of homeland security when either the costs or the benefits are difficult to quantify or are not valued in monetary terms.

- *Management selection*: The three components face different challenges in this area, because each has different types of alternatives available in making decisions. The Coast Guard has the most direct control over security efforts; it can, for example, decide what protective measures to take with its own assets, and it has authority over other stakeholders to implement the Maritime Transportation Security Act of 2002. Its challenges lie mainly in what has already been discussed above—strengthening methods for risk assessment and alternatives evaluation and integrating this effort with the annual cycle of program review—so that management can make the most informed decisions about these efforts. ODP affects security efforts less directly; it can only consider facilities that have applied for grants, and it has no direct authority over port facilities in general, as does the Coast Guard. ODP has worked with the Coast Guard to receive its input into the grant application process. One challenge is to consistently apply criteria for management selection in a more transparent way. IAIP faces the most challenges in this area, because once it makes recommendations about how to prioritize assets on a national scale, it is largely dependent on the actions of others to carry them out and, particularly for owners and operators of private infrastructure, is dependent to a large degree on persuasion, market forces, or the work of regulatory agencies that have authority over key infrastructure, to ensure that protective measures are in place.

- *Implementation and monitoring*: Particularly for the Coast Guard and ODP, we have been able to identify instances in which the components have moved aggressively to improve their risk management approaches—and to continue doing so. Particularly with its recent setback on its RAMCAP methodology, IAIP is considerably behind these two components in implementing any kind of risk management approach. To move forward, it must overcome more basic problems with assessing risks and alternatives.

Observation Four: In the Long Term, Progress Rests Heavily on a Level of Coordination That Has Yet to Be Demonstrated

In the long term, progress will become increasingly dependent on how well the nation's homeland security risk management effort is coordinated. We have identified and reported on some notable improvements in coordination at the port level, through such mechanisms as intelligence fusion and coordination centers, local area maritime security committees, and interagency operational centers.[1] Replicating such coordination among DHS agencies and with state, local, and industry stakeholders is key.

Currently, various assessment approaches are being used, and in many ways, these approaches are neither consistent nor comparable. Our work at IAIP, the Coast Guard, and ODP showed examples of these inconsistencies. For example, IAIP's initial plans called for treating all threat scenarios as equally likely to happen, while the Coast Guard and ODP are attempting to integrate the likelihood of various threat scenarios into their analysis vulnerabilities. The danger in using different methods is that if agencies develop systems and methodologies without some overall coordination, they may end up with redundant or incompatible systems that have little or no ability to inform one another. Even more important, these systems may provide decision makers with unreliable or incomplete data on how to allocate resources and protect the American people in a cost-effective way. Absolute compatibility is likely impossible given the multiple stakeholders at the federal, state, local, and industry levels. For example, owners and operators of critical infrastructure may value and act on risks differently than the Coast Guard and IAIP. Having a common risk management framework is a key consideration for assuring that knowledge and data can be transferred to all stakeholders, while permitting stakeholders to value risks in different ways. Even if agencies and stakeholders were working in close cooperation, lack of coordination is likely only to exacerbate the problem. This is particularly true given the difficulty of the task and the limited availability of federal risk management guidance.

Until now, having such inconsistencies may have seemed less important than just getting risk management efforts under way. To a degree, we found this was the case with the larger universe of homeland security actions: When we first began reviewing agency actions shortly after the

[1] GAO, *Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention*, GAO-05-394 (Washington, D.C.: Apr. 15, 2005).

September 11 attacks, we found agencies at work on many efforts, but signs of coordination problems were already apparent. Similarly, the risk management efforts that have been conducted to date appear fueled by a strong sense of the need to make some headway, with coordination and consistency a lesser concern. For example, IAIP, which is charged by statute with developing comprehensive assessments of the vulnerabilities of critical infrastructure and key resources, did not attempt to guide the Coast Guard's efforts in setting up a methodology for assessing port-specific risks. IAIP officials told us it was more important for the Coast Guard and other agencies to proceed with their risk assessment efforts than to delay starting, even though the officials recognized that these efforts might create approaches that would not mesh cleanly with the approach that IAIP would eventually develop. Given what has occurred to date, this course of action appears prudent, in that the Coast Guard has a considerable portion of a risk management system in place. If it had waited to begin until guidelines and policies had been set, it would still be waiting to start.

Now, however, the need for coordination is looming larger. IAIP has a significant role to play in this regard through its responsibility for providing agencies with guidance about risk management, but it has made limited progress. IAIP has been challenged in establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors, along with metrics and criteria for related programs and activities as called for by HSPD-7. While IAIP has coordinated its activities with entities such as ODP and the Coast Guard, it has yet to issue policies, guidelines, and methodologies as required by the directive. Making progress with regard to this challenge is key to an effective use of risk management resources, as the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets recognizes.

Guidance is also important when agencies integrate a concern for risk into the annual cycle of program and budget review. Doing so within an agency is a difficult task in that traditional ways of reviewing budgets and programs often rely on program data that call for continuing or expanding a program without examining the relative risks that are addressed with the funds that are expended. Shifting organizations toward this nexus of using risk-based data as part of annual management review cycles will take time, attention, and leadership. Even in agencies where much progress has been made in developing risk management techniques, integrating disparate systems such as risk management with budget and program management remains a long-term challenge. The Secretary of DHS has said that operations and budgets of its agencies will be reviewed through the prism of risk, but doing this is made difficult by the level of guidance and coordination that has been provided so far.

DHS has recently reorganized, and the consideration of whether its new organization will effectively implement its risk management responsibilities is an important one. At the time we conducted our review, risk management was the responsibility of IAIP. IAIP's risk management efforts were focused mainly on assessing and reducing the vulnerabilities that exist in and around specific facilities or assets. But DHS's responsibility is broader than this: besides assessing and reducing vulnerabilities at specific facilities, it also includes preventing attacks from occurring (and in the process protecting people and critical infrastructure) and responding to and recovering from natural disasters and acts of terrorism. This initial focus on vulnerabilities at specific assets had the potential of limiting DHS's ability to achieve the broader goal of using risk-based data as a tool to inform management decisions on all aspects of its missions. The Secretary of DHS has now moved risk management to a new Preparedness Directorate. Although, it is unclear how such a move could affect DHS's ability to carry out its risk management responsibilities, the new focus on preparedness may result in an emphasis that may go too far the other way—that is an emphasis on protection of specific assets and response and recovery at the expense of prevention. As DHS goes forward, the office in which the risk management responsibility resides should have a broad perspective across the department's entire mission as well as the necessary authority to hold DHS component agencies responsible for carrying out risk management activities in a coordinated and consistent manner.

Beyond DHS, integrating risk with existing systems for budget and program review is complicated by the fact that while IAIP has responsibility for coordinating this effort, IAIP and the Secretary of DHS are challenged because they must depend on others to follow risk management principles for programs and budgets at the other six major Departments or agencies that have been charged with assessing risks under HSPD-7. In regard to this situation, OMB has taken the position that this is what the Homeland Security Act and HSPD-7 call for and it does not play a role in this process. These conditions increase the uncertainty of implementing risk management across federal agencies in a way that informs program and budget review processes. Whether such practices will occur within the executive branch is unclear because of these organizational barriers.

Recommendations for Executive Action

To strengthen individual agency efforts to implement a risk management approach to homeland security activities, we recommend that the Secretary of Homeland Security direct the Undersecretary for IAIP to undertake the following three actions:

- As required by presidential directive, establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors, along with metrics and criteria for related programs and activities and develop a timetable for completing such guidance. Such policies and guidance should address the issue of integrating risk management systems into existing systems of program and budget review.
- As DHS continues to review its organizational structure, work with the Secretary's office to determine which office is best suited to help ensure that the responsibility for risk management policy and implementation has a broad enough perspective on all elements of risk, including threats, as well as the necessary authority to coordinate with DHS component agencies and hold them accountable for risk management activities.
- Work with the Office of Management and Budget to examine options for holding departments and agencies accountable for integrating risk management for homeland security programs and activities into the annual cycle of program and budget review.

Agency Comments and Our Evaluation

In commenting on a draft of chapter 5, DHS, including IAIP, generally concurred with the recommendations. In regard to our observation that there is a long-term need for guidance and coordination, DHS noted that as part of the department's second-stage review, a six-point agenda has been created to ensure that policies, operations, and structures are best aligned to address potential threats. This agenda is a major step in the right direction, and as we observe in this chapter, much work remains to be done to translate this goal into actions.

DHS agrees that the application of risk management to domestic terrorism has no precedent, and that the probabilities and consequences of terrorist acts are difficult to predict. DHS also concurred with our observation that the scope of establishing a risk management framework—a former IAIP Directorate responsibility—across the federal government is immense. DHS acknowledges that IAIP's progress has been limited in part because its risk assessment responsibilities span broad sectors of the nation's infrastructure rather than seaports alone. DHS also submitted written comments under separate cover and we revised the report where appropriate. Written comments from DHS are in appendix II.

Appendix I: A Risk Management Framework

This appendix describes how we developed the risk management framework and how we used it to evaluate activities related to homeland security and combating terrorism. The framework is intended to be a starting point for risk management activities and will likely evolve as processes mature and lessons are learned. A glossary is included at the end of this appendix.

General Lack of Uniform Guidance on Risk Management

Although the Homeland Security Act and subsequent strategies advocate the use of risk management to protect the nation's critical infrastructure and key resources, they did not define how this was to be accomplished. Homeland Security Presidential Directive 7 (HSPD-7) directed the Secretary of the Department of Homeland Security (DHS) to establish uniform policies, approaches, guidelines, and methodologies integrating federal infrastructure protection and risk management activities. However, no further direction or guidance as to the course of action has been forthcoming.

The ability to anticipate future happenings and to choose among alternatives lies at the heart of risk management and provides us with a guide, based on good management practices and supported by established internal controls that can enhance decision making. Although risk management has long been used for assessing risk in some sectors, such as environmental issues, health care, finance, and the insurance industry, the application of risk management principles to the homeland security area is relatively new. The many areas and activities under homeland security provide untested and difficult challenges because the source of the risk is an intelligent adversary with whom there exists little domestic experience. As a result, the probabilities and consequences of a terrorist attack are difficult to predict. In spite of this high degree of uncertainty and the knowledge that not all risk can be eliminated, enhancing protection from known or potential threats can help prevent or mitigate adverse events.

Methodology for Developing a Risk Management Framework

Given that there is no established universally agreed upon set of requirements or processes for a risk management framework specifically related to homeland security and combating terrorism, we developed a framework that would be applicable by reviewing, analyzing, and synthesizing several sources of information.

We began by reviewing current risk literature and previous GAO reports and testimonies.[1] We consulted the Government Performance and Results Act (GPRA) of 1993; the Government Auditing Standards, 2003 Revision, GAO's Standards for Internal Control in the Federal Government (November 1999); guidance from the Office of Management and Budget (OMB); the work of the President's Commission on Risk Management; consulting papers; and the enterprise risk management approach of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. In addition, we consulted with experts in the fields of risk management, risk modeling, and terrorism. We reviewed numerous frameworks from industry, government, and academic sources.

We synthesized information from these numerous government, industry, and academic sources in developing our risk management framework. The framework was field-tested on several GAO reviews. The draft framework was then reviewed by three academic experts in risk management. No substantial changes to the draft framework were recommended.

A Risk Management Framework

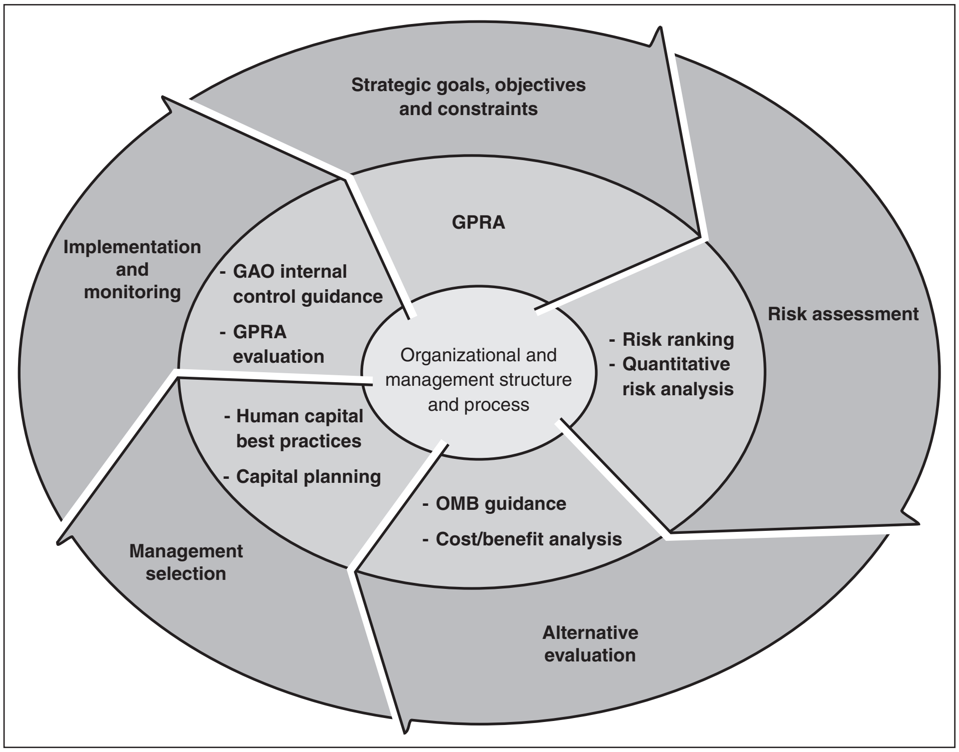
The framework should be considered to be a starting point in a field that is evolving, and the entire cycle of risk management activities should be viewed as a goal. The phases contained in the framework are

- strategic goals, objectives, and constraints;
- risk assessment;
- alternatives evaluation;
- management selection; and
- implementation and monitoring.

[1] GAO, *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, GAO/NSIAD-98-74 *(Washington, D.C.: April 1998); Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004); *Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain*, GAO-04-598T (Washington, D.C.: Mar. 23, 2004); and *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington, D.C.: Mar. 31, 2004).

The framework has been developed so that individual phases of the approach, such as risk assessment, do not become ends in themselves, but provide a full cycle of related activities, from strategic planning through implementation and monitoring. The process is dynamic, and although the various phases appear linear, new information can be entered at any phase. The framework can be used to inform agency officials and decision makers of the basic components of a risk management system or can be used as a stand-alone guide. Figure 4 illustrates our risk management framework and some sources of criteria, such as GAO best practices, Office of Management and Budget circulars, GAO guidance on internal controls, and the Government and Performance Act of 1993 and their link with management processes. While statistical methods and risk-ranking approaches frequently underlie risk assessment approaches, different application areas tend to develop their own terminologies and their own logical sequences for the cause of risk.

Figure 4: Sources of Evaluation Criteria Associated with Risk Management Phases


Strategic goals, objectives and constraints
GPRA
Implementation and monitoring
- GAO internal control guidance
- GPRA evaluation
Risk assessment
- Risk ranking
- Quantitative risk analysis
Organizational and management structure and process
- Human capital best practices
- Capital planning
- OMB guidance
- Cost/benefit analysis
Management selection
Alternative evaluation

Source: GAO.

The risk management framework is designed to be flexible, in that the approach may be applied at various organizational levels ranging from that of a department level of a multiagency organization down to that of a specific project or program.

Because there is no one uniformly accepted approach to risk management, terms and activities may differ across applications. However, any approach that omits the substance of the steps shown in figure 4 is likely to have material weaknesses. Table 11 summarizes the phases of our risk management framework and provides examples of elements contained in those phases.

Table 11: A Risk Management Framework

Phase	Description	Example of elements
Strategic goals, objectives, and constraints	Addresses what the strategic goals are attempting to achieve and the steps needed to attain those results	• Overall results desired, i.e., “end state” • Hierarchy of strategic goals and subordinate objectives related to those goals • Specific activities to achieve results • Priorities, milestones, and outcome-related performance measures • Limitations or constraints that affect outcomes
Risk assessment	Addresses identification of key elements of potential risks so that countermeasures can be selected and implemented to prevent or mitigate their effects	• Analysis of threat gained from available sources (This threat information will be used to develop scenarios. See below.) • Estimation of vulnerability of an asset based on standards, such as • Availability/predictability • Accessibility • Countermeasures in place, and • Target hardness • Identification of consequence of a terrorist attack on a specific asset and criticality, or the relative importance, of the asset involved
Alternatives evaluation	Addresses the evaluation of alternative countermeasures to reduce risk being considered with associated costs	• Specific countermeasure(s) to reduce risk • Use of external sources to improve decision making such as consultation with experts and threat scenarios • Cost-benefit analysis of countermeasure(s)
Management selection	Addresses where resources and investments will be made based on alternatives evaluation and other management criteria, such as availability of funds	• Management’s preferences and value judgments associated with expenditure of countermeasures and funds, such as distribution of antiterrorism measures over assets • Organizational risk tolerance • Resource allocations • Documentation of decisions, including rationale
Implementation and monitoring	Addresses how countermeasures will be applied and mechanism to keep security measures updated	• Implementation of countermeasures according to strategy • Periodic testing of countermeasures • Linkages to other risk management strategies, state, local, or private entities (horizontal) • Linkages to other strategies, departmental and national (vertical) • Mechanisms for alterations in system based on current threat data • Periodic evaluation for assessing efficiency and effectiveness of program

Source: GAO.

The following sections provide more detail on the five phases of our risk management framework.

Strategic Goals, Objectives, and Constraints

This phase addresses what the strategic goals are attempting to achieve and the steps needed to attain those results, including milestones and performance measures to permit measurement of progress toward those goals. Ideally, management decisions should be made in the context of a strategic plan, with clearly articulated goals and objectives that flow from the plan. Strategic goals at the highest level could be considered an "end-state" followed by a logical hierarchy of major goals and subordinate objectives composed of clear, concise, measurable activities and timelines to achieve results and ensure accountability. An organization's program or plan and risk planning documents should address risk-related issues that are central to its mission. Our work related to the Government Performance and Results Act of 1993 has produced guidance that identifies risk for the congressional oversight of federal agencies' strategic plans.[2] The consideration of risk in strategic planning may be incorporated into planning documents or into specific management strategies.

Currently, it is difficult to translate plans and actions into a clear sense of how we are progressing in making our nation more secure. One reason is that homeland security efforts, in general, lack clear goals with corresponding performance measures to evaluate progress toward these goals.[3] As others, such as the Gilmore Commission, have stated, a continuing problem for homeland security has been the lack of clear strategic guidance about the definition and objectives of preparedness.[4]

Risk management allows entities to operate more effectively in environments of uncertainty by providing the discipline and structure in which to address these issues, since risk management is not an end in itself, but an important component of an entity's management process. As such, risk management is interrelated with, among other things, an entity's

[2] GAO, *Agencies' Strategic Plans under GPRA: Key Questions to Facilitate Congressional Review*, GAO/GGD-10.1.16 (Washington, D.C.: May 1, 1997).

[3] GAO, *Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains*, GAO-02-610 (Washington, D.C.: June 7, 2002).

[4] The Gilmore Commission (also known as the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction), *Forging America's New Normalcy* (Arlington, Virginia: Dec. 15, 2003).

governance, performance management, and internal controls. The process of risk management provides the rigor and structure 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. This process enables entities to enhance their capability to identify potential adverse events, assess risks, and establish integrated responses. Further, this phase in the planning process would include support and buy-in from upper levels of management and stakeholders. Acceptance for concepts of the model from this group provides the groundwork for future discussions.

Finally, various constraints may have an impact on risk management plans. Some constraints may be imposed by statute, higher-level policy, budget, or other factors beyond management's control and may vary with the scale of the application. Managers at different levels within an organization will have different degrees of flexibility to institute risk management countermeasures. An important constraint for federal agencies, such as DHS, is the role that Congress plays in authorizing and funding programs. For example, Congress may direct specific actions affecting how agencies allocate funding.

Risk Assessment

This phase addresses the process of evaluating the threats and vulnerabilities of assets so that countermeasures might be instituted to prevent or mitigate risks. Threat, in the risk management model, concerns the probability that a specific type of attack will be initiated against a specific target. It includes any circumstance or event with the potential to cause loss or damage to the asset. Although agencies may not have enough information to identify and characterize all threats related to their assets, known or imagined adverse events would be characterized in some detail. Effective threat analysis is dependent on an understanding of an adversary's intention, motivation, historical data, and capability to damage. An additional crucial component of risk assessment is vulnerability, that is, any weakness that an adversary can exploit to harm or damage the asset. An asset may be highly vulnerable to one mode of attack but have a low level of vulnerability to another, depending on a variety of factors, such as countermeasures already in place. While consequence concerns the result of an adverse event on a particular asset, criticality is the asset's relative importance to the entity. A criticality assessment identifies and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy, as a basis for identifying which structures or processes are relatively more important to protect from attack. Criticality assessments are important because they provide, in combination with the framework's threat and risk assessments, the basis for prioritizing which assets require greater protection relative to finite resources and provide information for later stages in the risk management process. Risk assessments should utilize the most appropriate subject matter experts in assessing the components of risk. When dealing with Bayesian probability estimates, this is critical.[5] In addition, mathematical constructs must be chosen carefully, specifically tailoring approaches in the context of uncertainty and data quality.

Alternative Evaluation

This phase addresses the evaluation of risk reduction methods by consideration of countermeasures or countermeasure systems and the costs and benefits associated with them. Ideally, a risk management framework would include an evaluation of a risk assessment as a valid decision support tool to establish and prioritize a risk management strategy. Furthermore, a strategy might include risk management consultants and decision-making tools, such as software that simulates a particular type of attack. Information developed in previous phases would inform decisions.

Specific countermeasures would be considered and prioritized based on a number of factors, such as the degree of risk reduction they afford and the cost and difficulty to implement them. Risk assessment may give guidance to implementing countermeasures or countermeasure systems that may be used for more than one critical asset, or to prevent, mitigate, or respond to multiple adverse events occurring simultaneously. In addition, external risk consultants can be advantageous at this phase in terms of creating a variety of countermeasure options. While external reviewers cannot ensure the success of a plan, they can increase the probability of selecting the most effective countermeasures for the least cost because of their expertise in the area. Further, risk scenarios might also provide valuable information pertaining to an entity's ability to respond to a terrorist event, evaluate its coordination with other entities, identify problems, and institute corrective action.

Finally, a risk management strategy should include a cost-benefit analysis of countermeasure options as they are a critical element of alternatives

[5] See Yacov Y. Haimes, *Risk Modeling, Assessment, and Management*, 2nd ed. (Hoboken, New Jersey: Wiley and Sons, 2004).

evaluation. Major regulatory actions or capital investments of federal expenditures generally require a cost-benefit or cost-effectiveness approach.[6] This approach can be useful in evaluating alternatives, since it links the benefits from risk-reducing countermeasures to the costs associated with them. In the development of such analyses, quantitative impacts affecting both costs and benefits are, to the extent possible, identified in monetary terms.

While the core OMB guidance for evaluating countermeasures for budgetary and regulatory purposes focuses on monetary cost-benefit evaluation, OMB is essentially silent when costs and benefits cannot be easily quantified or monetized. Costs that are not generally estimated or included in monetary terms include opportunity costs, that is, the value of opportunities forgone because resources are applied to antiterrorism countermeasures. These costs are most controversial when considered in areas such as public service programs or services curtailed or cancelled. Benefits are usually measured in terms of the risk reduction they provide. They are considered in terms of the overall effectiveness of the countermeasures with respect to the estimated vulnerabilities.

Management Selection

This phase addresses such issues as determining where resources and investments will be made, the sources and types of resources needed, and where those resources would be targeted. Management's active participation in this phase is important as decisions are of necessity influenced by the preferences and value judgments of agency leadership. For example, some managers will prefer to concentrate countermeasures on a relatively few critical assets, while others may value distributional impacts, that is, to distribute resources over a wide variety of assets. Ideally, a risk management strategy would also identify appropriate mechanisms to allocate resources, such as grants based on identified needs. Furthermore, a key factor in the selection of risk reducing measures is risk tolerance, the level of comfort management has with various levels of risk. This tolerance may change over time, depending on new information, changes in financial constraints, and attitude toward risk. The risk management strategy, with stakeholder input, will identify what constitutes an acceptable level of risk for assets and how resources are delegated.

[6] Executive Order 12866 and circulars A-4 and A-94 apply to regulatory actions, and circulars A-11 (sect. 7), A-94, and A-130 apply to capital investments.

The risk management strategy reflects consideration as to which risks should be managed immediately and to what extent, and which risks can be deferred and addressed at a later time. Milestones and timelines for implementation are important elements that allow evaluating the extent to which progress is being made toward achieving goals. It also illustrates the degree of protection that can be obtained and places security and costs in perspective. The documentation of management decisions, including the rationales that support the decisions, will provide valuable information for future adjustments.

Implementation and Monitoring

This phase addresses the degree to which risk management strategies contain internal controls and performance measurement guidelines. In addition to implementing countermeasures, it may also include implementing new organizational policies and procedures, as well as human, physical, and technical controls. Countermeasures would be initiated in accordance with the timelines in the risk management schedule.

Monitoring and evaluation include, when and where appropriate, external peer review, testing and validation of countermeasures, evaluating the effects of these actions on future operation, and identifying unintended consequences. GAO has also discussed the importance of these activities as they ensure actions are taken to address risks.

Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.[7] Internal controls help to ensure that procedures are documented and maintained.

Difficulties Applying a Risk Management Framework

Risk management represents a unique set of challenges. Developing such a framework is designed to guide the actions of management to prepare for and respond to adverse events in an environment of uncertainty. As applied to homeland security, the ability to determine the likelihood of terrorism-related events occurring and quantifying the resulting outcomes is balanced against the benefit as protection (security) provided at an acceptable cost.

[7] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1, (Washington, D.C.: November 1999).

Generally, a major difficulty in executing and implementing a risk management system occurs because of what is commonly called decision uncertainty, that is, the assumed goal of minimizing risk does not have a common meaning.[8] For example, minimizing risk is based on values, the measure of risk, and the comparison of values and risk. Decision uncertainty arises when there is controversy or ambiguity concerning how to compare and weight social objectives. Three major sources of decision uncertainty are

- Risk measurement—although the selection of risk measurement is both an art and a science, it must be technically correct as well as both valid and meaningful.
- The social cost of risk—in order to make different risks comparable, various risks often have to be quantified into comparable quantities and placing values on cost and benefits involves judgments.
- The quantification of social values—uncertainty surrounds the level of risk that is acceptable or can be tolerated. That is, how much money is to be spent on protection meaning risk reduction and what is the cost in terms of opportunities forgone because of finite resources. This value is dependent upon determining society's risk attitude or tolerance and may change over time.

Coordination activities suggest that for the results of a risk management system to be meaningful and useful, all related agencies should be using similar methods. If agencies' methods are not compatible, then comparisons between agencies become difficult and sector or national risk assessments becomes less reliable. In our earlier work, we concluded that a structured, systematic approach to risk management offers the best assurance that activities designed to protect the homeland and combat the effects of terrorism will produce the most effective and efficient results.[9] Specific difficulties implementing risk management systems are contained in chapters 2, 3, and 4.

[8] For a more detailed discussion on this topic, see Yacov Y Haimes, *Risk Modeling, Assessment, and Management*, 2nd ed. (Hoboken, New Jersey: Wiley and Sons, 2004).

[9] See for example, GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington, D.C.: Mar. 31, 2004); *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: Oct. 31, 2001); and *Key Elements of a Risk Management Approach*, GAO-02-150T (Washington, D.C.: Oct. 12, 2001).

Glossary of Risk Management Terms

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

- *Asset*—any person, facility, material, information, or activity that has a positive or symbolic value. An asset may have a value to an adversary as well as to its owner, although the nature and magnitude of these values may differ. Assets may be categorized or combined in many ways; examples are people, information, equipment, facilities, operations, and activities.

- *Benefit*—net outcome, usually translated into monetary terms; a benefit may include both direct and indirect effects.

- *Consequence*—the expected worse case or reasonable worse case impact of a successful attack. The consequence to a particular asset can be evaluated when threat and vulnerability are considered together. This loss or damage may be long- or short-term in nature.

- *Cost*—input, both direct and indirect.

- *Cost-benefit analysis*—part of the management decision-making process in which the costs and benefits of each countermeasure alternative are compared and the most appropriate alternative is selected. Costs include the price paid for tangible materials and the ongoing operational costs associated with implementing the countermeasures. Benefits are expressed in terms of the amount of risk reduction based on the overall effectiveness of the countermeasure with respect to the assessed vulnerabilities.

- *Countermeasure*—any action taken or physical equipment used principally to reduce or eliminate one or more vulnerabilities. The cost of a countermeasure is usually expressed in monetary terms but may include nonmonetary costs such as reduced operational effectiveness, unfavorable working conditions, adverse publicity and political consequences.

- *Criticality assessment*—identifies and evaluates an entity's assets or operations on the basis of a variety of factors, including the importance of an asset or function and the significance of a system in terms of national security, economic activity, and public safety. A criticality assessment provides the basis for determining which assets require greater or special protection relative to finite resources.

- *Impact*—the amount of loss or damage that can be expected from a successful attack on an asset. Loss may be monetary, but may include loss of lives and destruction of a symbolic structure.

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

- *Opportunity cost*—the value of opportunities forgone.

- *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, activities, and operations. The principal classes of risk from terrorism are to the general public, targets of symbolic value, organizational, governmental, and societal infrastructure, cyber and physical infrastructure, and economic sectors and structures.

- *Risk assessment*—the process of qualitatively or quantitatively determining the probability of an adverse event and the severity of its impact on an asset. It is a function of threat, vulnerability, and consequence. A risk assessment may include scenarios in which two or more risks interact to create a greater or lesser impact. A risk assessment provides the basis for the rank ordering of risks and for establishing priorities for applying countermeasures.

- *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 and its negative impact. Risk management addresses risk before mitigating action, as well as the risk that remains after countermeasures have been taken.

- *Scenario*—the combination of weapon and attack mode on a specific target or critical asset (for example, the release of sarin gas in a subway train).

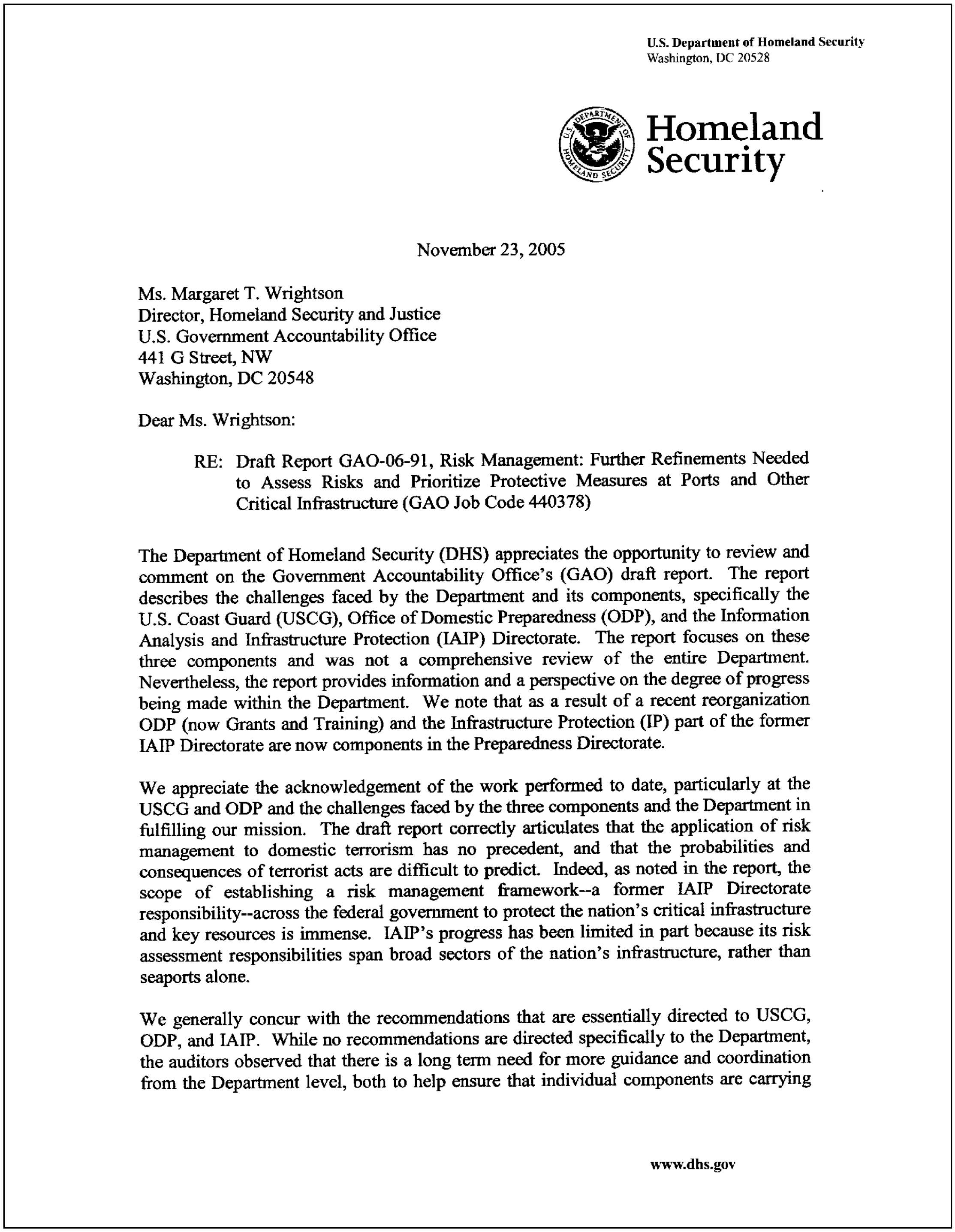
- *Threat*—an indication of the likelihood that a specific type of attack will be initiated against a specific target or class of targets. It may include any indication, circumstance, or event with the potential to cause the loss of or damage to an asset. It can also be defined as an adversary's intention and capability to undertake actions that would be detrimental to a valued asset.

- *Threat assessment*—-the identification and evaluation of adverse events that can harm or damage an asset. A threat assessment includes the probability of an event and the extent of its lethality. Threats may be present at the global, national, or local level.

- *Vulnerability*—-the probability that a particular attempted attack will succeed against a particular target or class of targets.

- *Vulnerability assessment*—-the identification of weaknesses in physical structures, personal protection systems, processes or other areas that may be exploited. A vulnerability assessment identifies inherent states and the extent of their susceptibility to exploitation relative to the existence of any countermeasures.

Appendix II: Comments from the Department of Homeland Security



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

Homeland
Security

November 23, 2005

Ms. Margaret T. Wrightson
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Wrightson:

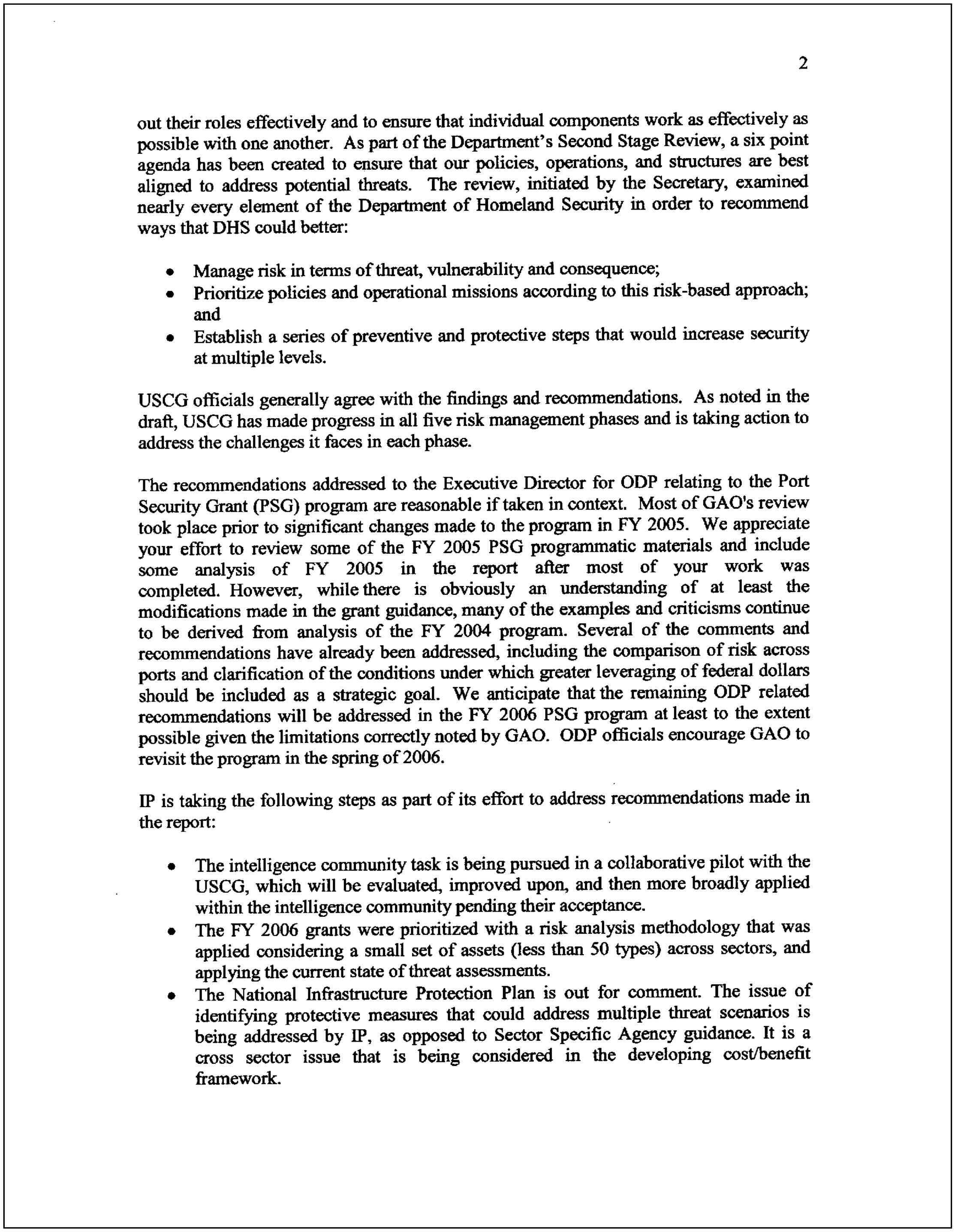
RE: Draft Report GAO-06-91, Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure (GAO Job Code 440378)

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the Government Accountability Office's (GAO) draft report. The report describes the challenges faced by the Department and its components, specifically the U.S. Coast Guard (USCG), Office of Domestic Preparedness (ODP), and the Information Analysis and Infrastructure Protection (IAIP) Directorate. The report focuses on these three components and was not a comprehensive review of the entire Department. Nevertheless, the report provides information and a perspective on the degree of progress being made within the Department. We note that as a result of a recent reorganization ODP (now Grants and Training) and the Infrastructure Protection (IP) part of the former IAIP Directorate are now components in the Preparedness Directorate.

We appreciate the acknowledgement of the work performed to date, particularly at the USCG and ODP and the challenges faced by the three components and the Department in fulfilling our mission. The draft report correctly articulates that the application of risk management to domestic terrorism has no precedent, and that the probabilities and consequences of terrorist acts are difficult to predict. Indeed, as noted in the report, the scope of establishing a risk management framework--a former IAIP Directorate responsibility--across the federal government to protect the nation's critical infrastructure and key resources is immense. IAIP's progress has been limited in part because its risk assessment responsibilities span broad sectors of the nation's infrastructure, rather than seaports alone.

We generally concur with the recommendations that are essentially directed to USCG, ODP, and IAIP. While no recommendations are directed specifically to the Department, the auditors observed that there is a long term need for more guidance and coordination from the Department level, both to help ensure that individual components are carrying

www.dhs.gov



out their roles effectively and to ensure that individual components work as effectively as possible with one another. As part of the Department's Second Stage Review, a six point agenda has been created to ensure that our policies, operations, and structures are best aligned to address potential threats. The review, initiated by the Secretary, examined nearly every element of the Department of Homeland Security in order to recommend ways that DHS could better:

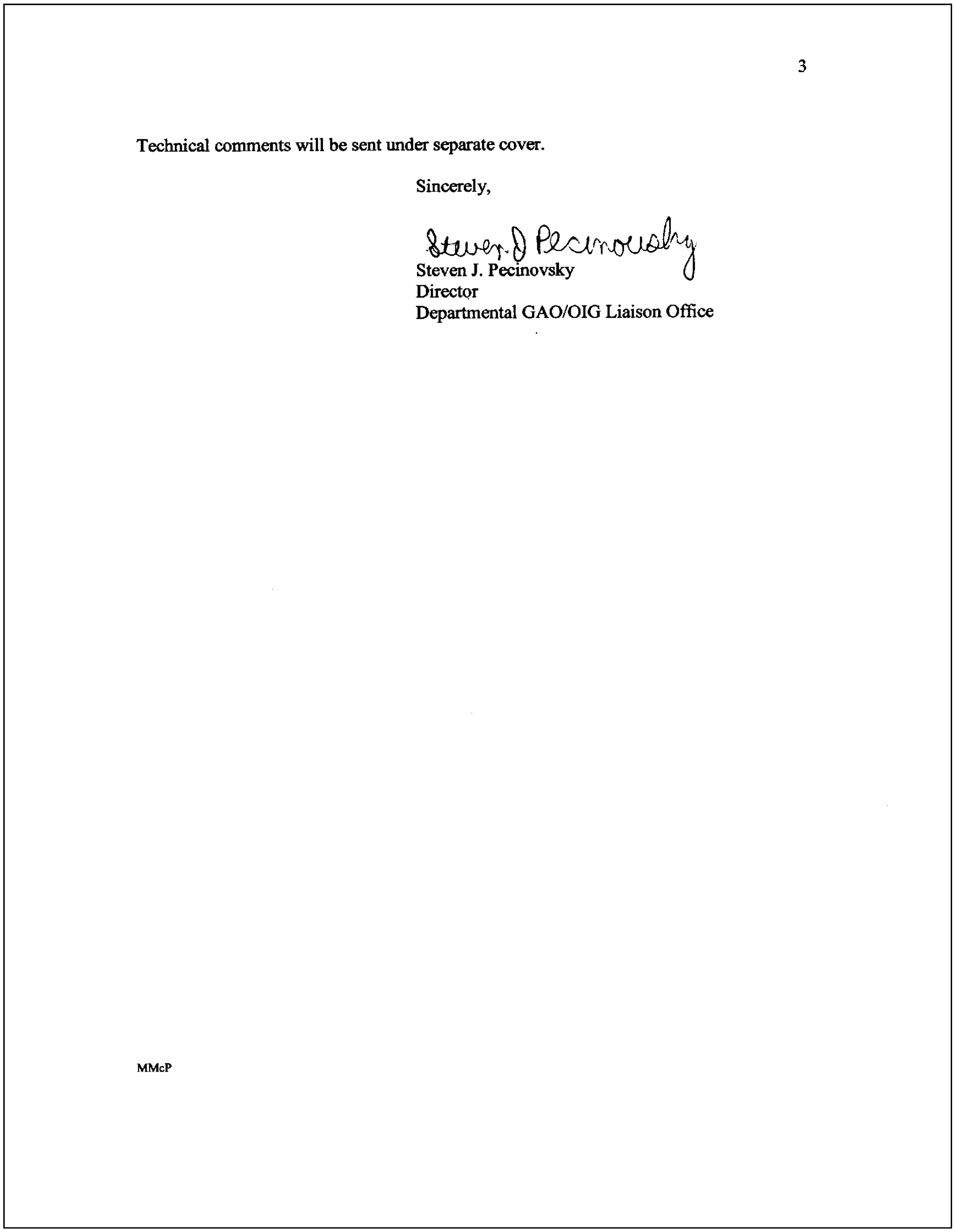
- Manage risk in terms of threat, vulnerability and consequence;
- Prioritize policies and operational missions according to this risk-based approach; and
- Establish a series of preventive and protective steps that would increase security at multiple levels.

USCG officials generally agree with the findings and recommendations. As noted in the draft, USCG has made progress in all five risk management phases and is taking action to address the challenges it faces in each phase.

The recommendations addressed to the Executive Director for ODP relating to the Port Security Grant (PSG) program are reasonable if taken in context. Most of GAO's review took place prior to significant changes made to the program in FY 2005. We appreciate your effort to review some of the FY 2005 PSG programmatic materials and include some analysis of FY 2005 in the report after most of your work was completed. However, while there is obviously an understanding of at least the modifications made in the grant guidance, many of the examples and criticisms continue to be derived from analysis of the FY 2004 program. Several of the comments and recommendations have already been addressed, including the comparison of risk across ports and clarification of the conditions under which greater leveraging of federal dollars should be included as a strategic goal. We anticipate that the remaining ODP related recommendations will be addressed in the FY 2006 PSG program at least to the extent possible given the limitations correctly noted by GAO. ODP officials encourage GAO to revisit the program in the spring of 2006.

IP is taking the following steps as part of its effort to address recommendations made in the report:

- The intelligence community task is being pursued in a collaborative pilot with the USCG, which will be evaluated, improved upon, and then more broadly applied within the intelligence community pending their acceptance.
- The FY 2006 grants were prioritized with a risk analysis methodology that was applied considering a small set of assets (less than 50 types) across sectors, and applying the current state of threat assessments.
- The National Infrastructure Protection Plan is out for comment. The issue of identifying protective measures that could address multiple threat scenarios is being addressed by IP, as opposed to Sector Specific Agency guidance. It is a cross sector issue that is being considered in the developing cost/benefit framework.



3

Technical comments will be sent under separate cover.

Sincerely,

Steven J. Pecinovsky

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

MMcP

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Margaret T. Wrightson (415) 904-2200

Stephen L. Caldwell (202) 512-9610

Staff Acknowledgments

In addition to the persons named above, David Alexander, Neil Asaba, Nancy A. Briggs, Christine Davis, Scott Farrow, Kevin Heinz, Emily S. Pickrell, Albert Schmidt, Stan Stenersen, April Thompson, and L. James Valverde made key contributions to this report.

Related GAO Products

Critical Infrastructure Protection

Critical Infrastructure Protection: Challenges in Addressing Cybersecurity. GAO-05-827T. Washington, D.C.: July 19, 2005

Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities. GAO-05-434. Washington, D.C.: May 26, 2005.

Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security. GAO-05-33. Washington, D.C.: January 14, 2005.

Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices. GAO-05-49. Washington, D.C.: November 30, 2004.

U.S. Postal Service: Physical Security Measures Have Increased at Some Core Facilities, but Security Problems Continue. GAO-05-48. Washington, D.C.: November 16, 2004.

Drinking Water: Experts' Views on How Federal Funding Can Best Be Spent to Improve Security. GAO-04-1098T. Washington, D.C.: September 30, 2004.

Financial Market Preparedness: Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters. GAO-04-984. Washington, D.C.: September 27, 2004.

Nuclear Regulatory Commission: Preliminary Observations on Efforts to Improve Security at Nuclear Power Plants. GAO-04-1064T. Washington, D.C.: September 14, 2004.

U.S. Postal Service: Better Guidance Is Needed to Ensure an Appropriate Response to Anthrax Contamination. GAO-04-239. Washington, D.C.: September 9, 2004.

Public Key Infrastructure: Examples of Risk and Internal Control Objectives Associated with Certification Authorities. GAO-04-1023R. Washington, D.C.: August 10, 2004.

Combating Terrorism: DOD Efforts to Improve Installation Preparedness Can Be Enhanced with Clarified Responsibilities and Comprehensive Planning. GAO-04-855. Washington, D.C.: August 9, 2004.

Homeland Security: Transformation Strategy Needed to Address Challenges Facing the Federal Protective Service. GAO-04-537. Washington, D.C.: July 14, 2004.

Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors. GAO-04-780. Washington, D.C.: July 9, 2004.

Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation. GAO-04-376. Washington, D.C.: June 28, 2004.

National Nuclear Security Administration: Key Management Structure and Workforce Planning Issues Remain as NNSA Conducts Downsizing. GAO-04-545. Washington, D.C.: June 25, 2004.

Nuclear Security: Several Issues Could Impede Ability of DOE's Office of Energy, Science, and Environment to Meet the May 2003 Design Basis Threat. GAO-04-894T. Washington, D.C.: June 22, 2004.

Information Security: Information System Controls at the Federal Deposit Insurance Corporation. GAO-04-630. Washington, D.C.: May 28, 2004.

Posthearing Questions Related to Fragmentation and Overlap in the Federal Food Safety System. GAO-04-832R. Washington, D.C.: May 26, 2004.

Terrorism Insurance: Effects of Terrorism Risk Insurance Act of 2002. GAO-04-720T. Washington, D.C.: April 28, 2004.

Nuclear Security: DOE Needs to Resolve Significant Issues before It Fully Meets the New Design Basis Threat. GAO-04-623. Washington, D.C.: April 27, 2004.

Terrorism Insurance: Implementation of the Terrorism Risk Insurance Act of 2002. GAO-04-307. Washington, D.C.: April 23, 2004.

Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors. GAO-04-699T. Washington, D.C.: April 21, 2004.

Homeland Security: Federal Action Needed to Address Security Challenges at Chemical Facilities. GAO-04-482T. Washington, D.C.: February 23, 2004.

Posthearing Questions from the September 17, 2003, Hearing on "Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: The Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness." GAO-04-300R. Washington, D.C.: December 8, 2003.

Security: Counterfeit Identification Raises Homeland Security Concerns. GAO-04-133T. Washington, D.C.: October 1, 2003.

Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened. GAO-03-752. Washington, D.C.: September 4, 2003.

Nuclear Security: DOE Faces Security Challenges in the Post September 11, 2001, Environment. GAO-03-896TNI. Washington, D.C.: June 24, 2003.

Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program. GAO-03-471. Washington, D.C.: May 30, 2003.

Information Security: Progress Made, but Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures. GAO-03-564T. Washington, D.C.: April 8, 2003.

Homeland Security: EPA's Management of Clean Air Act Chemical Facility Data. GAO-03-509R. Washington, D.C.: March 14, 2003.

Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown. GAO-03-439. Washington, D.C.: March 14, 2003.

Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants. GAO-03-414. Washington, D.C.: February 12, 2003.

Potential Terrorist Attacks: More Actions Needed to Better Prepare Critical Financial Markets. GAO-03-468T. Washington, D.C.: February 12, 2003.

Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants. GAO-03-251. Washington, D.C.: February 12, 2003.

High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures. GAO-03-121. Washington, D.C.: January 1, 2003.

Combating Terrorism: Actions Needed to Guide Services' Antiterrorism Efforts at Installations. GAO-03-14. Washington, D.C.: November 1, 2002.

Homeland Security: Department of Justice's Response to Its Congressional Mandate to Assess and Report on Chemical Industry Vulnerabilities. GAO-03-24R. Washington, D.C.: October 10, 2002.

Building Security: Interagency Security Committee Has Had Limited Success in Fulfilling Its Responsibilities. GAO-02-1004. Washington, D.C.: September 17, 2002.

Chemical Safety: Emergency Response Community Views on the Adequacy of Federally Required Chemical Information. GAO-02-799. Washington, D.C.: July 31, 2002.

Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed. GAO-02-918T. Washington, D.C.: July 9, 2002.

Information Security: Corps of Engineers Making Improvements, but Weaknesses Continue. GAO-02-589. Washington, D.C.: June 10, 2002.

Security Breaches at Federal Buildings in Atlanta, Georgia. GAO-02-668T. Washington, D.C.: April 30, 2002.

National Preparedness: Technologies to Secure Federal Buildings. GAO-02-687T. Washington, D.C.: April 25, 2002.

Diffuse Security Threats: Technologies for Mail Sanitation Exist, but Challenges Remain. GAO-02-365. Washington, D.C.: April 23, 2002.

Terrorism Insurance: Rising Uninsured Exposure to Attacks Heightens Potential Economic Vulnerabilities. GAO-02-472T. Washington, D.C.: February 27, 2002.

Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks. GAO-01-1168T. Washington, D.C.: September 26, 2001.

Combating Terrorism: Actions Needed to Improve DOD Antiterrorism Program Implementation and Management. GAO-01-909. Washington, D.C.: September 19, 2001.

Critical Infrastructure Protection: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities. GAO-01-1132T. Washington, D.C.: September 12, 2001.

Maritime Security

Coast Guard: Progress Being Made on Addressing Deepwater Legacy Asset Condition Issues and Program Management, but Acquisition Challenges Remain. GAO-05-757. Washington, D.C.: July 22, 2005.

Coast Guard—Electronic Certification Procedures. B-302789. Washington, D.C.: July 6, 2005

Coast Guard: Preliminary Observations on the Condition of Deepwater Legacy Assets and Acquisition Management Challenges. GAO-05-651T. Washington, D.C.: June 21, 2005.

Maritime Security: Enhancements Made, but Implementation and Sustainability Remain Key Challenges. GAO-05-448T. Washington, D.C.: May 17, 2005.

Coast Guard: Preliminary Observations on the Condition of Deepwater Legacy Assets and Acquisition Management Challenges. GAO-05-307T. Washington, D.C.: April 20, 2005.

Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention. GAO-05-394. Washington, D.C.: April 15, 2005.

Coast Guard: Observations on Agency Priorities in Fiscal Year 2006 Budget Request. GAO-05-364T. Washington, D.C.: March 17, 2005.

Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention. GAO-05-17. Washington, D.C.: January 14, 2005.

Coast Guard: Station Readiness Improving, but Resources Challenges and Management Concerns Remain. GAO-05-161. Washington, D.C.: January 31, 2005.

Port Security: Planning Needed to Develop and Operate Maritime Worker Identification Card Program. GAO-05-106. Washington, D.C.: December 10, 2004.

Maritime Security: Better Planning Needed to Help Ensure an Effective Port Security Assessment Program. GAO-04-1062. Washington, D.C.: September 30, 2004.

Maritime Security: Partnering Could Reduce Federal Costs and Facilitate Implementation of Automatic Vessel Identification System. GAO-04-868. Washington, D.C.: July 23, 2004.

Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security. GAO-04-838. Washington, D.C.: June 30, 2004.

Coast Guard: Station Spending Requirements Met, but Better Processes Needed to Track Designated Funds. GAO-04-695. June 14, 2004.

Coast Guard: Key Management and Budget Challenges for Fiscal Year 2005 and Beyond. GAO-04-636T. Washington, D.C.: April 7, 2004.

Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection. GAO-04-557T. Washington, D.C.: March 31, 2004.

Coast Guard Programs: Relationship between Resources Used and Results Achieved Needs to Be Clearer. GAO-04-432. Washington, D.C.: March 22, 2004.

Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers. GAO-04-325T. Washington, D.C.: December 16, 2003.

Posthearing Questions Related to Aviation and Port Security. GAO-04-315R. Washington, D.C.: December 12, 2003.

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.

Coast Guard: Challenges during the Transition to the Department of Homeland Security. GAO-03-594T. Washington, D.C.: April 1, 2003.

Transportation Security: Post-September 11th Initiatives and Long-Term Challenges. GAO-03-616T. Washington, D.C.: April 1, 2003.

Coast Guard: Comprehensive Blueprint Needed to Balance and Monitor Resource Use and Measure Performance for All Missions. GAO-03-544T. Washington, D.C.: March 12, 2003.

Homeland Security: Challenges Facing the Coast Guard as It Transitions to the New Department. GAO-03-467T. Washington, D.C.: February 12, 2003.

Coast Guard: Strategy Needed for Setting and Monitoring Levels of Effort for All Missions. GAO-03-155. Washington, D.C.: November 12, 2002.

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

Combating Terrorism: Preliminary Observations on Weaknesses in Force Protection for DOD Deployments through Domestic Seaports. GAO-02-955TNI. Washington, D.C.: July 23, 2002.

Risk Management

Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts. GAO-05-851. September 9, 2005

Homeland Security: Actions Needed to Better Protect National Icons and Federal Office Buildings from Terrorism. GAO-05-790. June 24, 2005.

Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges. GAO-05-327. Washington, D.C.: March 28, 2005.

Transportation Security: Systematic Planning Needed to Optimize Resources. GAO-05-357T. February 15, 2005

Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security. GAO-05-33. January 14, 2005.

Homeland Security: Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices. GAO-05-49. November 30, 2004

General Aviation Security: Increased Federal Oversight is Needed, but Continued Partnership with the Private Sector is Critical to Long-Term Success. GAO-05-144. November 10, 2004.

Air Traffic Control: System Management Capabilities Improved, but More Can Be Done to Institutionalize Improvements. GAO-04-901. August 20, 2004

Aviation Security: Challenges in Using Biometric Technologies. GAO-04-785T. May 19, 2004.

Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection. GAO-04-557T. March 31, 2004

Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain. GAO-04-598T. March 23, 2004.

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.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

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. Government Accountability 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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548