United States Government Accountability Office

GAO

Testimony before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, February 7, 2007

# HOMELAND SECURITY

# Applying Risk Management Principles to Guide Federal Investments

Statement of William O. Jenkins, Jr., Director
Homeland Security and Justice Issues

February 7, 2007

# HOMELAND SECURITY

# Applying Risk Management Principles to Guide Federal Investments

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-386T, a testimony before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

## Why GAO Did This Study

Since the terrorist attacks of September 11, 2001, and the subsequent creation of the Department of Homeland Security (DHS), the federal government has provided DHS with more than $130 billion in budget authority to make investments in homeland security. However, as GAO has reported, this federal financial assistance has not been guided by a clear risk-based strategic plan that fully applies risk management principles. This testimony discusses the extent to which DHS has taken steps to apply risk management principles to target federal funding for homeland security investments (1) in making grant allocations, (2) in funding transportation and port security enhancements, (3) in other DHS mission areas, and (4) at a strategic level across DHS. This testimony summarizes previous GAO work in these areas.

## What GAO Recommends

GAO has made numerous recommendations over the past 4 years aimed at enhancing DHS's use of risk management principles to guide homeland security investments in, for example, promoting all-hazards capabilities for catastrophic disasters, assessing customs and immigration systems for immigration enforcement, determining the potential for cyber attacks, and conducting modal transportation security research and development efforts.

www.gao.gov/cgi-bin/getrpt?GAO-07-386T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact William O. Jenkins Jr., at (202) 512-8757 or jenkinsWO@gao.gov.

## What GAO Found

Risk management, a strategy for helping policymakers make decisions about assessing risk, allocating resources, and taking actions under conditions of uncertainty, has been endorsed by Congress, the President, and the Secretary of DHS as a way to strengthen the nation against possible terrorist attacks. DHS has used risk management principles to invest millions of dollars at the state and local level as part of its Urban Area Security Initiative (UASI) grants. For fiscal year 2006, DHS adopted a risk management approach to determine which UASI areas were eligible for funding. For the fiscal year 2007 grant process, DHS made substantial changes to its 2006 risk assessment model, simplifying its structure, reducing the number of variables considered, and incorporating the intelligence community's assessment of threats in candidate urban areas. The fiscal year 2007 model considers most areas of the country equally vulnerable to attack; its analysis focuses on the expected impact and consequences of successful attacks occurring in specific areas.

DHS and the components of DHS responsible for transportation and port security have taken steps to apply risk management principles with varying degrees of progress. The Transportation Security Administration has not completed a methodology for assessing risk, and until the overall risk to the entire transportation sector is identified, it will be difficult to determine where and how to target limited resources to achieve the greatest security gains. The progress of each of DHS's three components responsible for port security varies according to organizational maturity and the complexity of its risk management task. The Coast Guard, created in 1915, was the most advanced in implementing a risk-based approach. Meanwhile, the Office for Domestic Preparedness (responsible for grants) and the Information Analysis and Infrastructure Protection Directorate (responsible for all sectors of the nation's critical infrastructure) were brought to or established with DHS in 2003 and lagged behind the Coast Guard in applying risk management to port security.

Other DHS mission areas GAO has assessed include border security, immigration enforcement, immigration services, critical infrastructure protection, and science and technology; the extent to which a risk management approach has been implemented in each area varies.

While DHS has called for using risk-based approaches to prioritize its resource investments, and for developing plans and allocating resources in a way that balances security and freedom, DHS has not comprehensively implemented a risk management approach—a difficult task. However, adoption of a comprehensive risk management framework is essential for DHS to assess risk by determining which elements of risk should be addressed in what ways within available resources.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing to discuss the Department of Homeland Security's (DHS) efforts to apply risk management principles to its investments in homeland security. The terrorist attacks of September 11, 2001, introduced our nation to threats posed by enemies very different from those the nation has faced before—terrorists such as al Qaeda, willing and able to attack us in our cities and homes. These new enemies used tactics designed to take advantage of our nation's vulnerabilities, many of which reflect our relatively open society and individual freedoms. The consequences of those attacks have been far reaching and unprecedented. In addition, events such as the tsunami that struck Indonesia and Sri Lanka, and Hurricanes Katrina and Rita reminded our nation of the need to consider all potential risks—natural, accidental, and man-made. Assessing and responding to these threats, vulnerabilities, and consequences are the fundamental elements of a risk management approach.[1] While simple to state in principal, applying risk management is difficult in practice, in part because assessing threats is an uncertain process due to limited historical data on which to assess the probability of various types of risk. A risk management approach entails a continuous process of mitigating risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives.

In the years since the 9/11 attacks, the nation has begun confronting the nation's risks at the federal, state, local, and private levels. At home, the Congress enacted legislation creating DHS and strengthening other security measures in law enforcement and border and transportation security. Since September 11, 2001, and the subsequent creation of DHS, the federal government has provided the department with more than $130 billion in budget authority to make investments in homeland security. However, as we have reported, these investments have not been guided by a clear risk-based strategic plan that applies risk management principles.

As the Comptroller General and the Secretary of DHS have previously testified, we cannot afford to protect everything against all threats—choices must be made about how best to allocate available resources

[1]GAO, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: Oct. 31, 2001).

given the risks we face. While risk-based allocation decisionmaking is still evolving, GAO has proposed a systematic risk management approach for allocating resources that reflects an assessment of threats, vulnerabilities, and the potential consequences of terrorist attacks and other risks. In assessing the challenges faced by the nation for the 21st Century, the Comptroller General has asked the question, "What criteria should be used to target federal funding for homeland security in order to maximize results and mitigate risk within available resource levels?"

Today, I am here to discuss the extent to which DHS has taken steps to apply risk management principles to target federal funding for homeland security investments (1) in making homeland security grant allocations, (2) in funding transportation security enhancements, (3) in funding port security enhancements, (4) in other DHS mission areas, and (5) at a strategic level across the department.

My comments are based on GAO's historical body of work on risk management principles, including:

- *Strategic Budgeting: Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities*, GAO-05-357T, February 15, 2005; and
- *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T, October 31, 2001.

In addition, my testimony draws on issued GAO reports and testimonies addressing DHS's use of risk management to make homeland security investments in specific mission areas, for example:

- *Homeland Security Grants: Observations on Process DHS Used to Allocate Funds to Selected Urban* Areas, GAO-07-381R, February 7, 2007;
- *Passenger Rail Security Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-07-225T, January 18, 2007; and
- *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91, December 15, 2005.

This work was conducted according to generally accepted government auditing standards.

## Summary

Risk management, a strategy for helping policymakers make decisions about assessing risk, allocating resources, and taking actions under conditions of uncertainty, has been endorsed by Congress, the President, and Secretary of DHS as a way to strengthen the nation against possible terrorist attacks. DHS has called for using risk-based approaches to prioritize its resource investments, and for developing plans and allocating resources in a way that balances security and freedom. The purpose of risk management is not to eliminate all risks; that is an impossible task. Rather, given limited resources, risk management is a structured means of making informed trade-offs and choices about how to use available resources effectively and monitoring the effect of those choices. Risk management is a continuous process. It includes the assessment of threats, vulnerabilities, and consequences, with actions taken to reduce or eliminate one or more of these elements of risk. Risk management includes a feedback loop that continually incorporates new information, such as changing threats or the effect of actions taken to reduce or eliminate identified threats, vulnerabilities, and/or consequences. Thus, risk is not a static concept. Because we have imperfect information for assessing risks, there is a degree of uncertainty in the information used for risk assessments (e.g., what the threats are and how likely are they to be realized). As a result, it is inevitable that assumptions and policy judgments must be used in risk analysis and management. It is important that key decisionmakers understand the basis for those assumptions and policy judgments and their effect on the results of the risk analysis and the resource decisions based on that analysis. Full adoption of a risk management framework is essential for DHS to assess risk by determining which elements of risk should be addressed in what ways within available resources. A risk management approach can also inform decisions on setting relative homeland security priorities and making spending decisions. To do so, DHS must carefully weigh the benefit of homeland security endeavors and allocate resources where the benefit of reducing risk is worth the additional cost. The results of DHS risk management efforts in specific areas varies.

*Grant Allocations:* Today, we issued a report, listed above, on DHS's use of risk assessments in distributing the Urban Area Security Initiative (UASI) grants. In that report, we describe how DHS's use of risk management principles has evolved over 4 years of investing millions of dollars at the state and local level to enhance homeland security. During this period, DHS has provided about $14 billion in federal funding to

states, localities, and territories through its grants under the Homeland Security Grant Program (HSGP).[2] From fiscal year 2003 through 2005, DHS used an approach for assessing risk based largely on indicators such as population density combined with threat assessments. For fiscal year 2006, DHS adopted a more sophisticated risk assessment approach to determine both (1) which UASI areas were eligible for funding, based on their potential risk relative to other areas, and (2) in conjunction with a new effectiveness assessment, the amount of funds awarded to eligible areas. As described by DHS officials, the fiscal year 2007 grant process included substantial changes to the 2006 risk assessment model, simplifying its structure, reducing the number of variables considered, and incorporating the intelligence community's assessment of threats for all candidate urban areas, which was used to assign the areas to one of four tiers, according to their relative threat, with Tier I being those at highest threat. In fiscal years 2006 and 2007, the risk assessment process has been used to assess threat, vulnerability, and the consequences of various types of successful attacks for each urban area assessed. One difference in 2007 is that DHS considered most areas of the country equally vulnerable to attack, given the freedom of movement within the United States. It focused its analysis on the expected impact and consequences of successful attacks occurring in specific areas of the country, given their population, population density, and assets. The risk assessment process is not perfect, is evolving, and of necessity involves professional judgments, such as assigning the weights to be used for specific factors in the risk assessment model. Although DHS has made progress in developing a method of assessing relative risk among urban areas, DHS officials have said that they cannot yet assess how effective the actual investments from grant funds are in enhancing preparedness and mitigating risk because they do not yet have the metrics necessary to do so.

*Transportation Security:* Regarding the use of risk management approaches to guide investments in transportation security, we reported last month that DHS and the Transportation Security Administration (TSA) have taken steps to apply risk management principles to all modes of transportation with varying degrees of progress. However, our work for

[2]Prior to fiscal year 2003, funding to urban areas was provided under the Nunn-Lugar-Domenici Domestic Preparedness Program, which was administered by the Department of Defense starting in fiscal year 1997, and later the Department of Justice during fiscal years 2001 and 2002. Other grants under the HSGP include the State Homeland Security Program, Law Enforcement Terrorism Prevention Program, and Citizen Corps Program, among others.

that report also showed that both DHS and TSA should take additional steps to help ensure that the risk management efforts under way clearly and effectively identify priority areas for security-related investments in rail and other transportation modes. TSA has not yet completed its methodology for determining how the results of threat, vulnerability, and criticality (the severity of the consequences that may follow a successful attack) assessments will be used to identify and prioritize risks to passenger rail and other transportation sectors, including air cargo, general aviation, and commercial airports. Until the overall risk to the entire transportation sector is identified, TSA will not be able to determine where and how to target limited resources to achieve the greatest security gains. Once risk assessments have been completed, it will be critical to be able to compare assessment results across all transportation modes and make informed, risk-based investment trade-offs. It is important that DHS complete its framework to help ensure that risks to all sectors can be analyzed and compared in a consistent way.

*Port Security:* In 2005, we reported on the risk management approaches used by three DHS components responsible for port security and critical infrastructure —the Coast Guard and two other DHS components that were within the Office for Domestic Preparedness (ODP) and the Information Analysis and Infrastructure Protection Directorate (IAIP) prior to DHS's August 2005 Second-Stage Review and departmental reorganization. We found that the Coast Guard had made the most progress in establishing a foundation for using a risk management approach; its next challenge was to further refine and enhance its approach. Specifically, we noted that the Coast Guard had made the greatest progress in conducting risk assessments—that is, evaluating individual threats, the degree of vulnerability, and the consequences of a successful attack. These assessments, however, were limited in their reliability and completeness, and we concluded that better coordination would be needed with the intelligence community so that analysts could develop models that better assess the relative probability of various threat scenarios. Our report also noted that ODP had made progress in applying risk management to the port security grant program, but like the Coast Guard, it also faced challenges across all phases of the risk management framework. For example, ODP had set broad risk management goals and had placed more emphasis on using risk-based data in its assessments, but at the time, it lacked performance measures showing what specific outcomes the program aimed to achieve and it still faced challenges in such matters as comparing grant applications across ports. Finally, IAIP—which had the broadest risk management responsibilities of the three components and faced the greatest challenges at the time of our review—

had made the least progress in carrying out its complex risk management activities. Its efforts were aligned with high-level strategic goals, but ways to measure performance in achieving these goals were not yet developed. We found IAIP was not as far along as ODP and the Coast Guard in conducting risk assessments, and while IAIP provided input to ODP for its risk assessment efforts, IAIP's risk assessment responsibilities spanned much broader sectors of the nation's infrastructure than seaports alone, making its assessment activities more difficult.[3]

*Other mission areas:* We have also assessed DHS's risk management efforts across a number of other mission areas in the years since the Department was established--including border security, immigration enforcement, immigration services, critical infrastructure protection, and science and technology—and found varying degrees of consideration and application of risk management principles in DHS's investments in homeland security. For example, we identified several problems with the process DHS uses to assess the risks posed by each of the visa waiver countries' continued participation in the program and concluded in a 2006 report that DHS had not taken critical steps to mitigate the risk of the use of stolen passports from visa waiver countries. In the area of immigration enforcement, we recommended in 2006 that DHS conduct comprehensive threat, vulnerability, and consequence risk assessments of the customs and immigration systems to identify the types of violations with the highest probability of occurrence and most significant consequences in order to guide resource allocation. Regarding immigration services, we reported in 2006 that United States Citizenship and Immigration Services had not yet developed a comprehensive risk management approach to identify the types of immigration benefits that are most vulnerable to fraud and the consequences of their exploitation. In terms of critical infrastructure, we reported in October 2006 that DHS guidance does not require sector-specific critical infrastructure protection plans to address how the risk assessments are being performed or how the most critical assets are being protected. We have also assessed DHS's efforts to protect critical information systems infrastructure and reported in September 2006 that DHS had initiated efforts to fulfill 13 key cybersecurity

[3]There are 17 sectors identified in the Interim National Infrastructure Protection Plan: agriculture, public health and healthcare, drinking water and wastewater treatment systems, energy, banking and finance, national monuments and icons, defense industrial base, information technology, telecommunications, chemical, transportation systems, emergency services, postal and shipping, dams, government facilities, commercial facilities, and nuclear reactors, materials, and waste.

responsibilities, but it had not fully addressed any of them. We have made numerous recommendations in this area over the last several years, including several which focus on the need to conduct threat and vulnerability assessments, develop a strategic analysis and warning capability for identifying potential cyber attacks, and protect infrastructure control systems. Finally, in the area of science and technology, we recommended in 2004 that DHS complete strategic plans for transportation security research and development programs and conduct risk assessments for all modes of transportation to guide research and development investment decisions. These and other related reports are listed in appendix I.

*Strategic Application of Risk Management Principles:* Although DHS has made varying degrees of progress in developing risk assessments and risk management approaches for specific programs, it has not comprehensively implemented a risk management approach across the department as a whole--a difficult task. 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. As our 2006 report on risk management at ports and other critical infrastructure concluded, as DHS's 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. Efforts to establish guidance to coordinate a risk-based approach across DHS components has been hampered by organizational restructuring. The challenges that remain are substantial and will take time, leadership, and attention to resolve. This is particularly true when risk management is viewed strategically—that is with a view that goes beyond assessing what the risks are, to the integration of risk into annual budget and program review cycles.

## Background

Risk management has been widely practiced for years in areas such 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 decisions on ways to reduce the likelihood that an adverse event will occur, and mitigate the negative impact of and ensure a speedy recovery from those that do. Achieving these goals involves making 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 where scarce resources will do the most good at narrowing gaps in security.

Homeland security is a broad term with connotations resulting from the September 11 attacks and other connotations resonating from the disaster created by Hurricane Katrina in August 2005. Risk management has applications for deliberate attacks of terror and natural disasters, such as hurricanes and earthquakes. My statement today examines the approach used by DHS to deal with both of these areas.

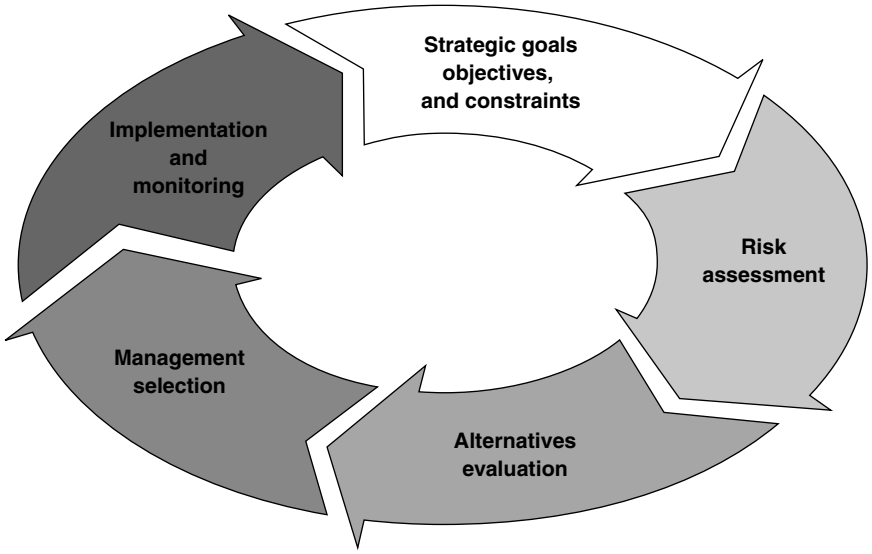
Risk management has received widespread support as a tool that can help inform decisions on how to protect the homeland. The Homeland Security Act of 2002 requires DHS to carry out a comprehensive assessment of risk related to vulnerabilities of critical infrastructure and key resources, notably (1) 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 resource allocation decisions. The President has issued policies directing the heads of seven major departments or agencies to assess risks. These policies have made DHS responsible for the national effort at protecting critical infrastructure and they call on DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating risk management within and across federal departments and agencies. In addition, risk management is one of the target capabilities DHS has established to measure state and local emergency preparedness and make homeland security investments in achieving the National Preparedness Goal. DHS's "Target Capabilities List" identifies risk management as one of four common capabilities for incident management—prevention, protection, response and recovery—for major events.

While there is widespread support for the use of risk management in homeland security programs, doing so is a complex task that has few precedents and until recently, little specific guidance. To provide a basis for examining efforts at carrying out risk management, we developed a

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

framework for risk management based on best practices and other criteria. The framework is divided into five 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 the results achieved (see figure 1). We used this framework to examine many of the programs that I discuss later in this statement. The application of risk management to homeland security is relatively new and the framework will likely evolve as processes mature and lessons are learned.

**Figure 1: Risk Management Framework**




Source: GAO.

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.

Risk management approaches have been applied to DHS's investments in state and local homeland security through the Homeland Security Grant Program (HSGP). The HSGP includes the Urban Area Security Initiative (UASI), the State Homeland Security Program, Law Enforcement Terrorism Prevention Program, and Citizen Corps Program. In fiscal year 2007, DHS has been appropriated funds to provide over $1.6 billion in federal funding to states, localities, and territories through the HSGP to prevent, protect against, respond to, and recover from acts of terrorism or other catastrophic events.

DHS components also use risk management principles to varying degrees to allocate funding to implement their homeland security missions. Key homeland security missions and the associated departmental agencies and organizations include

- *Emergency preparedness and response:* The Federal Emergency Management Agency (FEMA) prepares the nation for all hazards and coordinates the federal response and recovery efforts following any incident that requires federal support to state and local emergency responders. Under the statutorily mandated FEMA reorganization that is to take effect by March 31, 2007, FEMA is to include the Office of Grants and Training, which is responsible for allocating homeland security grants to states and localities, including the UASI and State Homeland Security grants. In addition, FEMA will be the responsible for implementing the National Preparedness Goal and other programs that are designed to enhance the nation's prevention, protection, response and recovery capabilities.
- *Transportation Security:* The Transportation Security Administration (TSA) is responsible for security for all modes of transportation and, while TSA's efforts have historically focused on aviation security due to the events of 9/11, increasing attention has been paid to surface transportation security as a result of more recent international terrorist attacks.
- *Maritime security:* The United States Coast Guard (USCG) is the lead federal agency for maritime homeland security. Key objectives of the nation's maritime security strategy are to prevent terrorist attacks and criminal or hostile acts, protect maritime-related population centers and critical infrastructures, minimize damage and expedite recovery, and safeguard the ocean and its resources.[5]

[5]Department of Homeland Security, The National Strategy for Maritime Security, September 2005.

- *Border Security:* U.S. Customs and Border Protection (CBP) was created to protect the nation's borders in order to prevent terrorists and terrorist weapons from entering or exiting the United States while facilitating the flow of legitimate trade and travel.
- *Immigration Enforcement:* Immigration and Customs Enforcement (ICE) was established to enforce immigration and customs laws and to protect the United States against terrorist attacks.
- *Immigration Services:* U.S. Citizenship and Immigration Services (USCIS) is responsible for the administration of immigration and naturalization adjudication functions and establishing immigration services policies and priorities. USCIS provides immigration benefits to people who are entitled to stay in the United States on a temporary or permanent basis.
- *Critical infrastructure and key assets protection:* The Directorate for Preparedness[6] is responsible for establishing uniform policies, approaches, guidelines, and methodologies to help ensure that critical infrastructure is protected, and using a risk management approach to coordinate protection efforts. The Directorate works with state, local, and private-sector partners to identify threats, determine vulnerabilities, and target resources where risk is greatest, thereby safeguarding our borders, seaports, bridges and highways, and critical information systems. The National Cyber Security Division is charged with identifying, analyzing, and reducing cyber threats and vulnerabilities, disseminating threat warning information, coordinating incident response, and providing technical assistance in continuity of operations and recovery planning.
- *Science and Technology:* The Directorate for Science and Technology (S&T Directorate) is the primary research and development arm of DHS. Its mission is to provide federal, state and local officials with the technology and capabilities to protect the homeland.

Since 2004, Congress has appropriated over $100 billion for DHS's homeland security efforts. For example, Congress has appropriated more than $30 billion in fiscal years 2006 and 2007 for some of the key components and agencies GAO has reviewed, as shown in table 1.

[6]Under the DHS reorganization that is to take effect on March 31, 2007, the Directorate for Preparedness is to become the National Protection and Program Directorate whose responsibilities are to include both infrastructure protection and risk management and analysis.

**Table 1: DHS Appropriation Amounts for selected components for Fiscal Years 2006 and 2007 (Dollars in Millions)**

| DHS component/agency | Fiscal year 2006 total | Fiscal year 2007 total |
|---|---|---|
| Citizenship and Immigration Services | $114 | $182 |
| Customs and Border Protection | 6,749 | 8,035 |
| Federal Emergency Management Agency | 8,986 | 2,511 |
| Immigration and Customs Enforcement | 3,483 | 3,958 |
| Preparedness Directorate | 4,056 | 4,018 |
| Science and Technology Directorate | 1,487 | 973 |
| Transportation Security Administration | 3,866 | 3,628 |
| U.S. Coast Guard | 8,056 | 8,316 |
| **Total for selected components** | **$36,797** | **$31, 621** |

Source: Congressional Research Service, RL33428, *Homeland Security Department: FY2007 Appropriations* (Washington, D.C.; Nov. 17, 2006).

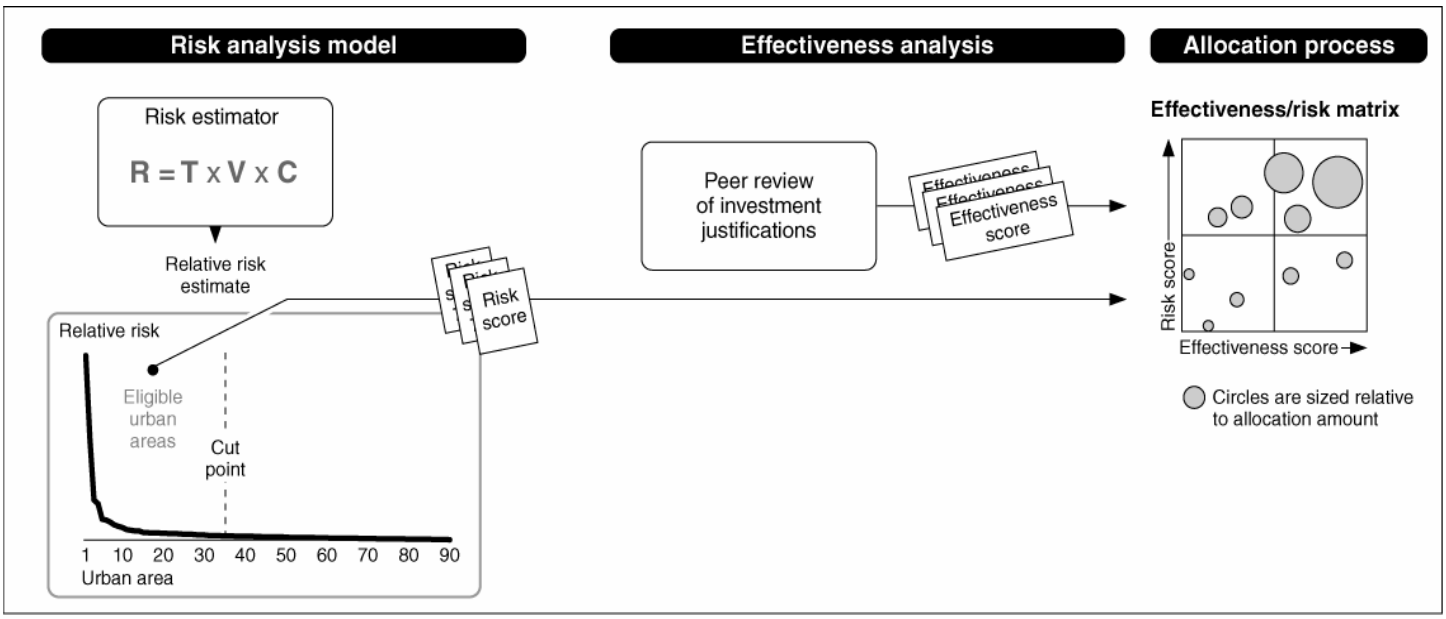
As the Comptroller General has repeatedly stated, our nation's fiscal policy is on an unsustainable course. Long-term budget simulations by GAO, the Congressional Budget Office (CBO), and others show that, over the long term, we face a large and growing structural deficit due primarily to known demographic trends and rising health care costs. Continuing on this unsustainable fiscal path will gradually erode, if not suddenly damage, our economy, our standard of living, and ultimately our national security. DHS is responsible for ensuring that the nation's annual investments of billions of dollars are targeted to the most efficient and effective uses using a sound, comprehensive risk management approach.

## DHS's Use of a Risk Management Approach to Guide Investments through the Homeland Security Grant Allocation Process Is Evolving

### DHS Uses a Risk-Based Approach in Distributing Urban Area Security Initiative Grants

Today, we issued a report on DHS's use of risk management in distributing the Urban Area Security Initiative (UASI) grants. For fiscal years 2006 and 2007, DHS has used risk assessments to identify urban areas that faced the greatest potential risk, and were therefore eligible to apply for the UASI grant, and based the amount of awards to all eligible areas primarily on the outcomes of the risk assessment and a new effectiveness assessment. Starting in fiscal year 2006, DHS made several changes to the grant allocation process, including modifying its risk assessment methodology, and introducing an assessment of the anticipated effectiveness of investments. DHS combined the outcomes of these two assessments to make funding decisions (see fig. 2.)

**Figure 2: Overview of DHS's UASI Grant Determination Process in Fiscal Year 2006**




Source: GAO analysis of DHS documents and information provided in interviews.

DHS used different risk assessment methodologies for the 2006 and 2007 UASI grant process, reflecting the evolving nature of its risk assessment approach. It is important to note that our understanding of the process is based principally on DHS officials' description of their process, including briefings, and limited documentation on the details on the actual data used and the methodology's application.

## Fiscal Year 2006 Grant Process

For fiscal year 2006, DHS's risk assessment included the three components we have identified as essential elements of an effective risk management approach—threat, vulnerability, and consequences—to estimate the relative risk of successful terrorist attacks to urban areas. DHS assessed risk from two perspectives, based on specific locations (asset-based) and based on areas of the country (geographic risk). To estimate asset risk, DHS assessed the intent and capabilities of an adversary to successfully attack an asset type, such as a chemical plant, dam, or commercial airport, using different attack scenarios (e.g., nuclear explosion or vehicle-borne improvised explosive device). DHS assessed geographic risk by approximating the threat, vulnerability, and consequences considering general geographic characteristics—mostly independent of the area's assets—using counts of data, such as reports of suspicious incidents, the

number of visitors from countries of interest, and population. In DHS's view, the estimates of asset-based risk and geographic risk are complementary and provided a "micro- and macro-" perspective of risk, respectively.

Because of data limitations and the inherent uncertainties in risk assessment, DHS officials had to apply policy and analytic judgments. For example, DHS made judgments about how to weight asset and geographic risk, how to identify the urban boundaries it used to estimate risk, and what data were sufficient to use in its risk estimates. DHS used this risk assessment to identify the eligibility cut point, which determined the number of urban areas that could apply for UASI funding in fiscal year 2006 and defined high-risk urban areas. According to DHS officials, the DHS Secretary selected a point that resulted in 35 eligible urban areas, which accounted for 85 percent of total related risk.

DHS also implemented a competitive process to evaluate the anticipated effectiveness of proposed homeland security investments by using peer reviewers--homeland security professionals from fields such as law enforcement and fire service. The peer reviewers scored the investments using criteria, such as regionalization, sustainability, and impact. For fiscal year 2006, DHS required urban areas to submit investment justifications as part of their grant application to assess the anticipated effectiveness of the various risk mitigation investments urban areas proposed. Reviewers on each panel assigned scores for six investment justifications, which were averaged to determine a final effectiveness score for each urban area. The criteria reviewers used to score the investment justifications included:

- relevance to the interim National Preparedness Goal,
- relevance to state and local homeland security plans,
- anticipated impact,
- sustainability, and
- regionalism.

The risk and effectiveness scores did not automatically translate into funding amounts, but rather, the scores were used in conjunction with final decisions on allocation amounts made by the Secretary of Homeland Security. To prioritize the allocation of funds DHS used the combined scores to assign eligible urban areas into four categories: Category I—higher risk, higher effectiveness; Category II—higher risk, lower effectiveness; Category III—lower risk, higher effectiveness; and Category IV—lower risk, lower effectiveness. DHS officials gave Category I the highest funding priority and Category IV the lowest funding priority. For

fiscal year 2006, once the amounts for each category were decided, DHS used a formula to determine the grant award for each urban area, giving the risk score a weight of 2/3 and the effectiveness score a weight of 1/3. The final funding decision resulted in 70 percent of UASI funding going to "higher risk" candidates in Categories I and II. DHS extended eligibility to an additional 11 "sustainment" urban areas that participated in the program in fiscal year 2005, but did not make the eligibility threshold in the 2006 risk assessment process.

One concern we identified during our review was that DHS had limited knowledge of how changes to its risk assessment methods, such as adding asset types and using additional or different data sources, affected its risk estimates. As a result, DHS had a limited understanding of the effects of the judgments made in estimating risk that influenced eligibility and allocation outcomes in fiscal year 2006. DHS leadership could make more informed policy decisions if provided with alternative risk estimates and funding allocations resulting from analyses of varying data, judgments, and assumptions. The Office of Management and Budget (OMB) offers guidelines for treatment of uncertainty in a number of applications, including the analysis of government investments and programs. These guidelines call for the use of sensitivity analysis to gauge what effects key sources of uncertainty have on outcomes. According to OMB, assumptions should be varied and outcomes recomputed to determine how sensitive analytical results are to such changes.[7] By applying these guidelines decisionmakers are better informed about how sensitive outcomes are to key sources of uncertainty. While DHS has indicated that it has performed some analyses, at this date it has not provided us with details on the extent of these analyses, how they were used, or how much they cost.

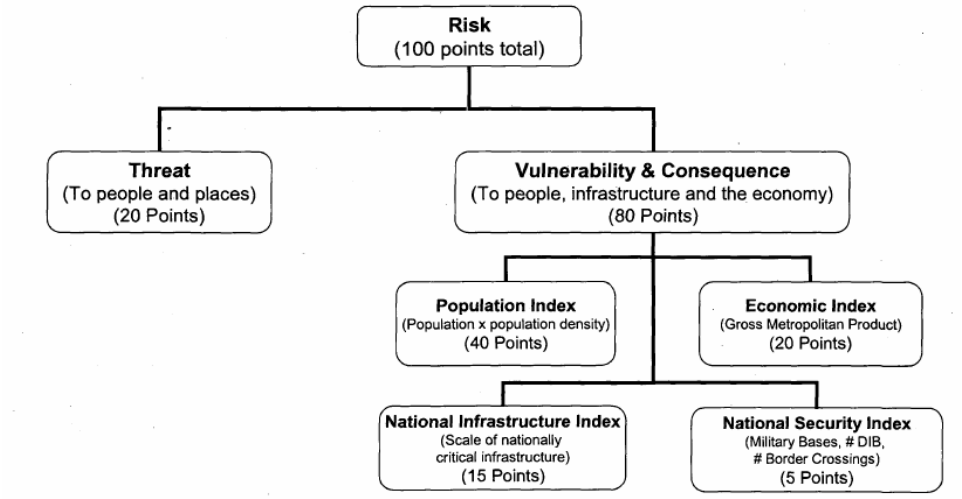
## Fiscal Year 2007 Process

The fiscal year 2007 process, as described by DHS officials, represents a continuing evolution in DHS's approach to its risk methodology for grant allocation. DHS officials said they will to continue to use the risk and effectiveness assessments to inform final funding decisions. For fiscal year 2007, DHS officials described changes that simplified the risk methodology, integrated the separate analyses for asset-based and geographic-based risk, and included more sensitivity analysis in determining what the final results of its risk analysis should be. DHS

[7]Office of Management and Budget, *Circular A-94: Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*, (Washington, D.C.: October 29, 1992)10-11.

officials said the primary goal was to make the process more transparent and more easily understood, focusing on key variables and incorporating comments from a variety of stakeholders regarding the fiscal year 2006 process. For the 2007 grant cycle, DHS no longer estimated asset-based and geographic risk separately, considered most areas of the country equally vulnerable to a terrorist attack, given freedom of movement within the nation, and focused on the seriousness of the consequences of a successful terrorist attack. As shown in figure 3, the maximum risk score possible for a given area was 100. Threat to people and places accounted for a maximum 20 points, and vulnerability and consequences for a maximum 80 points. In the fiscal year 2007 process the intelligence community for the first time assessed threat information for multiple years (generally, from September 11, 2001, forward) for all candidate urban areas and gave the Office of Grants and Training a list that grouped these areas into one of four tiers. Tier I included those at highest threat, relative to the other areas, and tier IV included those at lowest threat relative to the others.

**Figure 3: DHS's UASI Risk Assessment Methodology for Fiscal Year 2007**




Source: Department of Homeland Security, Office of Grants and Training.

Note: DIB is Defense Industrial Base.

According to DHS officials, the greatest concern was the impact of an attack on people, including the economic and health impacts of an attack. Also of concern was the quantity and nature of nationally critical infrastructure within each of the 168 urban areas assessed. In assessing

threat, vulnerability and consequences, DHS specifically wanted to capture key land and sea points of entry into the United States, and the location of defense industrial base facilities and nationally critical infrastructure facilities. The approximately 2,100 critical infrastructure assets included in the risk assessment were selected on the basis of analysis by DHS infrastructure protection analysts, sector specific agencies, and the states. These assets included some 129 defense industrial base assets. Assets were grouped into two tiers: (1) those that if attacked could cause major national or regional impacts similar to those from Hurricane Katrina or 9/11, and (2) highly consequential assets with potential national or regional impacts if attacked. Tier II included about 660 assets identified by state partners and validated by sector specific agencies. On the basis of Office of Infrastructure Protection analysis, Tier I assets were weighted using an average value three times as great as Tier II assets.

Throughout this process, a number of policy judgments were necessary, including what variables to include in the assessment, the points to be assigned to each major variable (e.g., threat, the population index, economic index, national infrastructure index, and the national security index) with an eye toward how these judgments affected outcomes. DHS officials noted that such judgments were the subject of extensive discussions, including among high-level officials. In addition, DHS officials said that they conducted more sensitivity analyses than was possible in the fiscal year 2006 process. DHS officials noted that because expert judgment was applied to the data and fewer variables were used in the current model, it was possible to track the effect of different assumptions and values on the ranking of individual urban areas. However, we have limited understanding of the sensitivity analyses that DHS conducted for the fiscal year 2006 and 2007 risk assessments because DHS has not provided us documentation on what analyses were conducted, how they were conducted, how they were used, and how they affected the final risk assessment scores and relative rankings.

Finally, DHS officials said that the effectiveness assessment process will be consistent with last year's process, although enhancements will be made based on feedback received; however, no final decision has been made on the weights to be given to risk and effectiveness for the allocation of the fiscal year 2007 grants. One modification to the effectiveness assessment will provide urban areas the opportunity to include investments that involve multiple regions. This can potentially earn an extra 5 percent to 8 percent on their final score. In addition, DHS may convene separate peer review panels to assess proposed investments for

these multi-regional investments. DHS has also offered applicants a mid-year review where applicants can submit their draft applications to DHS to obtain comments, guidance, or address questions that the grant may pose (such as little or unclear information on the anticipated impact of the investment on preparedness). As in the 2006 process, DHS officials have said that they cannot assess how effective these investments, once made, are in mitigating risk.

## DHS's Use of a Risk Management Approach for Transportation Security Investments Can Be Strengthened

Our past work examining TSA found that this DHS component has undertaken numerous initiatives to strengthen transportation security, particularly in aviation, and their efforts should be commended. However, we found that TSA could strengthen its risk-based efforts to include conducting systematic analysis to prioritize its security investments.[8] Although TSA has implemented risk-based efforts with many of its programs and initiatives, we have found—because of circumstances beyond TSA's control and a lack of planning—that TSA has not always conducted the systematic analysis needed to inform its decision-making processes and to prioritize security enhancements. For example, we found that TSA has not always conducted needed assessments of threats, vulnerabilities, and criticality in allocating its resources, and has not fully assessed alternatives that could be pursued to achieve efficiencies and potentially enhance security. Such planning could guide TSA in moving forward in its allocation of transportation resources both within aviation and across all transportation modes.[9]

Much of our work in the area of transportation security has focused on aviation and rail security, and our reviews have identified the need for a greater focus on, and application of, a risk management approach to guide investments in enhancing air cargo, general aviation, commercial airport, and passenger rail transportation security.

- *Air Cargo Security:* In October 2005, we reported that TSA had taken initial steps toward applying a risk-based management

[8]GAO, *Transportation Security: Systematic Planning Needed to Optimize Resources*, GAO-05-824T (Washington, D.C.: June 29, 2005).

[9]GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-06-181T (Washington, D.C.: Oct. 20, 2005) p.12; *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts* GAO-07-225T (Washington, D.C.: Jan. 18, 2007).

approach to address air cargo security.[10] In that report, we noted that, in November 2003, TSA completed an air cargo strategic plan that outlined a threat-based, risk management approach to secure the air cargo system by, among other things, targeting elevated risk cargo for inspection. TSA also completed an updated threat assessment in April 2005. However, we found that TSA had not yet established a methodology and schedule for completing assessments of air cargo vulnerabilities and critical assets—two crucial elements of a risk-based management approach without which TSA may not be able to appropriately focus its resources on the most critical security needs.

- *General Aviation Security:* In reporting on efforts to enhance general aviation security in 2004, we found that TSA had not conducted an overall systematic assessment of threats to, or vulnerabilities of, general aviation to determine how to better prepare against terrorist threats.[11] TSA had conducted limited vulnerability assessments at selected general aviation airports based on specific security concerns or requests by airport officials. TSA reported its intentions to implement a risk management approach to better assess threats and vulnerabilities of general aviation aircraft and airports and, as part of this approach, was developing an outline vulnerability self-assessment tool to be completed by individual airport managers. However, we noted limitations to the use of the self-assessment tool, and TSA had not yet developed a plan with specific milestones to implement the assessment, thereby making it difficult to monitor the progress of its efforts.

- *Commercial Airport Access Control and Perimeter Security:* In June 2004, we reported that TSA had not yet developed a plan to prioritize expenditures to ensure that funds provided have the greatest impact in improving the security of the commercial airport system. Through funding of a limited number of security enhancements, TSA had helped to improve perimeter and access control security at some airports. However, we concluded that,

[10]GAO, *Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security*, GAO-06-76 (Washington, D.C.: Nov. 2004).

[11]GAO, *General Aviation Security: Increased Federal Oversight Is Needed, but Continued Partnership with the Private Sector Is Critical to Long-Term Success*, GAO-05-144 (Washington, D.C.: Nov. 2004.)

without a plan to consider airports' security needs systematically, TSA could not ensure that the most critical security needs of the commercial airport system were identified and addressed in a priority order.[12] We will initiate work later this year to assess the steps TSA has taken to better prioritize its homeland security investments in this area.

- *Surface Transportation Security:* As we reported last month, DHS's Office of Grants and Training has developed and conducted risk assessments of passenger rail systems to identify and protect rail assets that are vulnerable to attack, such as stations and bridges.[13] TSA has also begun to conduct risk assessments, including a threat assessment of mass transit and passenger rail and assessments of individual critical rail assets. While TSA has begun to establish a methodology for determining how to analyze and characterize the risks identified, the agency has not completed a comprehensive risk assessment of the U.S. passenger rail system. Until TSA completes this effort, the agency will be limited in its ability to prioritize passenger rail assets and help guide security investment decisions about protecting them. Similarly, TSA has not yet conducted threat and vulnerability assessments of other surface transportation assets, which may adversely affect its ability to adopt a risk-based approach for prioritizing security initiatives within and across all transportation modes.

[12] GAO, *Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Control*, GAO-04-728 (Washington D.C.: June 2004) 16,18.

[13] GAO, *Passenger Rail Security Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-07-225T (Washington, D.C.: Jan. 18, 2007).

## DHS's Progress in Using a Risk Management Approach in Making Port Security Investments Can Be Linked to Each of Three Component's Organizational Maturity and Task Complexity

In December 2005, we reported that three DHS components responsible for port security or infrastructure protection varied considerably in their progress in developing a sound risk management framework for homeland security.[14] Our work reviewed the risk management approaches used by three DHS components prior to DHS's Second Stage Review and departmental reorganization:

- the Coast Guard, the lead federal agency for the security of the nation's ports;
- Office of Domestic Preparedness (ODP), the former DHS component responsible for administering federal homeland security assistance programs for states and localities, including the port security grant program, and
- the Information Analysis and Infrastructure Protection Directorate (IAIP), the former DHS component responsible for, among other things, identifying and assessing current and future threats to the homeland, mapping those threats against known vulnerabilities, and offering advice on preventive and protective action. This DHS component was responsible for cataloging key critical infrastructure, then analyzing various characteristics to prioritize this infrastructure, including those located at ports, for the entire nation.[15]

We found at that time that the varied progress reflected, among other things, each component's organizational maturity and the complexity of its task (see table 2). The Coast Guard, which was furthest along, is the component of longest standing, being created in 1915, while IAIP had came into being with the creation of the Department of Homeland Security in 2003. We found that IAIP had made the least progress. This DHS component was not only a new component but also has the most complex task: addressing not just ports but all types of infrastructure. Those DHS components that had a relatively robust methodology in place for assessing risks at ports were the Coast Guard and, what was at the time the Office for Domestic Preparedness (ODP), who awarded grants for port security projects. IAIP was still developing its methodology and had several setbacks in completing the task. We found that all three

[14] GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.; Dec. 15, 2006).

[15] ODP and the Infrastructure Protection part of the former IAIP Directorate are now components in the Preparedness Directorate.

components had much left to do. In particular, each component was limited in its ability to compare and prioritize risks. The Coast Guard and ODP were able to do so within a port but not between ports, and at that time, IAIP did not demonstrate that it could compare and prioritize risks either within or between all infrastructure sectors.

**Table 2: DHS Component Degree of Progress Implementing a Risk Management Framework by Organization Characteristics and Complexity of Task**

| 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.

## Coast Guard Progress Reflects Historical Focus on Risk Management Efforts

The Coast Guard was furthest along among the three components, reflecting in part where it stood in relationship to all three of these factors. It had 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. The Coast Guard implemented a port security risk assessment tool 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's Progress in Risk Management Reflected Its More Recent Initiation of Efforts and Organizational Role

At the time of our review, ODP had made somewhat less progress than the Coast Guard. Relative to the Coast Guard's progress, its progress reflected a later start, an organization with much less institutional maturity, and a different role from the Coast Guard's in that ODP provided 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 had come in the procedures recently adopted for the fiscal year 2005 grants. In moving toward risk management, ODP had 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 had port security as their focus, ODP's more limited scope of responsibility also had an effect on its risk management efforts. First, because ODP's role was to award grants that support federal priorities in port security, its progress in risk management depended to a degree on the progress made by other federal agencies in determining what their own port security performance measures should be. Second, ODP's funding priorities were subject to criteria other than risk, as the fiscal year 2004 grant awards demonstrated. 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.

## Lack of IAIP Progress in Risk Management Reflects In Part Its Broader Focus

Of the three components, IAIP was the least far along in its risk management efforts. All three factors have had an effect on this progress: IAIP had been at its task for a relatively short time; it was a new component; and relative to the Coast Guard and ODP, the scope of its efforts was 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 faced 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 extended well beyond the port-focused activities of the Coast Guard or ODP. (At the time, IAIP was responsible for conducting risk assessments for every critical infrastructure segment in the nation.) As demonstrated by the experience of its Risk Analysis and Management for Critical Asset Protection (RAMCAP) methodology for comparing risk across sectors, IAIP remained challenged in meeting that responsibility. Its lack of progress reflected 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 was unable at that time to provide adequate assurance to Congress or the country that the federal government was in a position to effectively manage risk in national security efforts. Steps have been small; by far, the biggest work is still yet to come.

## DHS Use of Risk Management in Making Investments in Other Mission Areas Varies by Degree and Application

We have assessed DHS's risk management efforts across a number of other mission areas in the 4 years since the department was established--including border security, immigration enforcement, immigration services, critical infrastructure protection, and science and technology—and found varying degrees of consideration and application of risk management principles in DHS's investments in homeland security.

*Border Security:* In 2006, as part of our work on border security, we issued a report assessing how DHS manages the risks of the Visa Waiver Program.[16] The Visa Waiver Program enables citizens of 27 countries to travel to the United States for tourism or business for 90 days or less without obtaining a visa. While there are benefits to the program in terms of facilitating travel for millions of people, inherent risks include barriers to border inspectors conducting in-depth interviews of travelers and the use of stolen passports from visa waiver countries. DHS had taken some action to mitigate the program's risks. For example, it had established a unit to conduct biennial reviews of the Visa Waiver Program as mandated by Congress in 2002. Yet stakeholders were not consulted during portions of the process, preparation for in-country site visits was not consistent, and the final reports were untimely. Further, the department had not established time frames and operating procedures regarding timely stolen passport reporting—a program requirement since 2002. DHS also had not issued clear reporting guidelines to the program's participating countries about reporting lost and stolen passport data.

*Immigration Enforcement:* In the area of immigration enforcement, we reported in 2006 that, while ICE had taken some initial steps to introduce principles of risk management into its operations, it had not conducted a comprehensive risk assessment of the customs and immigration systems to determine the greatest risks for exploitation, nor analyzed all relevant data to inform the evaluation of alternatives and allow officials to make risk-based resource allocation decisions.[17] We recommended that ICE conduct comprehensive risk assessments, including consideration of threats, vulnerabilities, and consequences, of the customs and immigration systems to identify the types of violations with the highest probability of

[16]GAO, *Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program*, GAO-06-854 (Washington, D.C.: July 2006).

[17]GAO, *Homeland Security: Better Management Practices Could Enhance DHS's Ability to Allocate Investigative Resources*. GAO-06-462T, (Washington, D.C.: March 2006).

occurrence and most significant consequences in order to guide resource allocation.

*Immigration Services:* In 2006, we reported that USCIS had not yet developed a comprehensive risk management approach to identify the types of immigration benefits that are most vulnerable to fraud and the consequences of their exploitation, monitored ongoing efforts to determine needed policy and procedural changes to reduce immigration benefit fraud, or sanctioned those who commit immigration benefit fraud to help deter them from committing future fraudulent acts.[18] We recommended that USCIS implement additional internal controls and best practices to strengthen its fraud control environment and that DHS develop a strategy for implementing a sanctions program.

*Critical Infrastructure:* As we reported in October 2006, DHS issued a National Infrastructure Protection Plan in June 2006 to serve as a road map for how DHS and other relevant stakeholders should use risk management principles to prioritize protection activities within and across sectors in an integrated, coordinated fashion.[19] However, we concluded that DHS guidance does not require the plans to address how the sectors are actually assessing risk and protecting their most critical assets. In September 2006, we reported that DHS had initiated efforts to address its responsibilities for enhancing the cybersecurity of information systems that are a part of the nation's critical infrastructure but had not fully addressed all 13 of its key responsibilities.[20] For example, while DHS had begun a variety of initiatives to fulfill its responsibility to develop an integrated public/private plan for Internet recovery, these efforts were not complete or comprehensive. Many of DHS's efforts lacked time frames for completion and the relationships among its various initiatives were not evident. We recommended that DHS (1) conduct threat and vulnerability assessments, (2) develop a strategic analysis and warning capability for identifying potential cyber attacks, (3) protect infrastructure control

[18]GAO, *Immigration Benefits: Additional Controls and a Sanctions Strategy Could Enhance DHS's Ability to Control Benefit Fraud*, GAO-06-259 (Washington, D.C.: March 2006).

[19]GAO, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, GAO-07-39 (Washington, D.C.: Oct. 2006).

[20]GAO, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity* GAO-06-1087T (Washington, D.C.: Sept. 13, 2006).

systems, (4) enhance public/private information sharing, and (5) facilitate recovery planning, including recovery of the Internet in case of a major disruption.

*Science and Technology:* In the area of science and technology, we reported in 2004 that DHS had not yet completed a strategic plan to identify priorities, goals, objectives, and policies for the research and development (R&D) of homeland security technologies.[21] We recommended that DHS complete a strategic R&D plan and ensure that this plan is integrated with homeland security R&D efforts of other federal agencies; complete strategic plans for transportation security research; and develop programs and conduct risks assessments for all modes of transportation to guide research and development investment decisions.

[21] GAO, *Homeland Security: DHS Needs a Strategy to Use DOE's Laboratories for Research on Nuclear, Biological, and Chemical Detection and Response Technologies*, GAO-04-653 (Washington, D.C.: May 2004).

## DHS Has Not Provided Guidance for a Coordinated Risk Management Approach and More Work Remains to be done in Carrying Out Such an Approach

### DHS Has Identified the Need for a Risk-based Approach, but Efforts to Develop Guidance to Coordinate Such an Approach Have Been Hampered by Organizational Restructuring

The need for 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, 2001, and the creation of DHS. Yet, this general acknowledgment has not been accompanied by the guidance necessary to make consistent use of risk management across DHS. The National Strategy for Homeland Security and DHS's strategic plan called for the use of risk-based decisions to prioritize DHS's resource investments regarding homeland security related programs. Although the Homeland Security Act and subsequent strategies call for 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. In addition, 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. As our 2006 report on risk management at ports and other critical infrastructure concluded, as DHS's 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.

Efforts to establish guidance to coordinate a risk-based approach across DHS components has been hampered by organizational restructuring. At the time we conducted our 2005 review of risk management for ports and other critical infrastructure, risk management was the responsibility of the Infrastructure Protection Office. The Infrastructure Protection Office'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.

In July 2005, the Secretary of DHS announced the department's Second Stage Review and reorganization, which had moved risk management to a new Preparedness Directorate. At the time of our work, we determined it was unclear how such a move could affect DHS's ability to carry out its risk management responsibilities, and were concerned that the new focus on preparedness could 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. To comply with certain requirements in the fiscal year 2007 DHS appropriation act, particularly with regard to FEMA, DHS is reorganizing, with some of the responsibilities of the Preparedness Directorate moving to FEMA. The Undersecretary for Preparedness is to become the Undersecretary for National Protection and Programs, retaining responsibility for risk management and analysis. The new structure is to take effect by March 31, 2007. As we noted in our past work, the office responsible for risk management 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.

## Over the Long-Term, More Work Remains to Be Done in Carrying Out a Risk-Based Approach

DHS has centered much attention on implementing risk management, but much more work remains to be done than has been accomplished so far. As discussed in the preceding sections, DHS components have made progress in applying risk management to varying degrees in guiding homeland security investments in state and local capabilities and in implementing their homeland security missions. The challenges that remain, however, are substantial and will take time, leadership, and attention to resolve. This is particularly true when risk management is viewed strategically—that is with a view that goes beyond what assessing the risks are and integrating a consideration for risk into annual budget

and program review cycles. In this way, DHS faces challenges in the following areas:

- Developing a way to compare and set priorities across different types of key infrastructure the Department is responsible for overseeing. While DHS components, such as TSA and the Coast Guard, have made progress in applying risk management to airports and seaports, challenges remain in making comparisons across assets and infrastructure within the transportation sector and in setting relative priorities. DHS has been challenged in establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection within the department, including metrics and criteria. While coordination occurs among the various components in the department, our work shows that components apply risk management in ways that are neither consistent nor comparable. The degree to which DHS uses common metrics, criteria, and approaches remains a management challenge.

- Coordinating efforts across the federal government. DHS plays a central role in guiding risk management activities across the federal government and much more work remains in offering policies, guidelines, and methodologies, including metrics and criteria, for the array of programs covered by Homeland Security Presidential Directives. Seven major departments or agencies are covered by the Directives, including the Departments of Defense, Energy, and Agriculture. DHS is developing a methodology to do this, but in the absence of this, these departments will use approaches that may not be compatible or may not be able to inform one another. Until such a methodology is in place, it will be impossible for DHS to make a determination of relative risks that could inform spending decisions.

- Integrating a concern for risk into other management systems, such as the annual cycle of budget and program review. A key aim of risk management is to inform decisions on setting relative priorities and on spending and ultimately to improve the quality of decisions made. Doing so, however, is difficult in that the 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. Additionally, DHS is challenged because it must depend on others to follow risk management principles at other federal departments or agencies that have also been called on to implement risk management.

Translating the concept of risk management into applications that are consistent and useful represents a major challenge for DHS as it moves from an organization that is in its early stages to one that is more organizationally mature. 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. Failure to address the strategic challenges in risk management could have serious consequences for homeland security. Until it does so, DHS is unable to provide adequate assurance to the Congress or the country that the federal government is in a position to effectively manage risk in national security efforts.

## Concluding Observations

Fully integrating a risk management approach into decision-making processes is challenging for any organization, and is particularly challenging for DHS, with its diverse set of responsibilities. But the basic goal across DHS homeland security programs is similar—to identify, prevent where possible, and protect the nation from risks of all types to people, property, and the economy. DHS has taken the first step in confronting this challenge by acknowledging the need for such an approach. It has taken further steps by incorporating risk management principles to at least some degree into making homeland security grant allocations, funding transportation and port security enhancements, and targeting federal funding across other DHS mission areas. However, much work remains to be done to implement a comprehensive risk management approach across DHS. We do not underestimate the challenge involved. Nevertheless, such a comprehensive implementation would place DHS in a better position to identify the threats that can and should be offset by limited resources. So that policymakers can make informed spending decisions, it is essential that policymakers fully understand the the assumptions and policy judgments that inform the risk analyses used for these decisions. A more comprehensive approach to risk management would also help the DHS components responsible for emergency preparedness, transportation, port security, and other mission areas to better protect our nation's assets. Without further attempts to address this incomplete work, DHS cannot assure the Congress or the public that federal funding is targeting the most critical risks.

Mr. Chairman and Members of the Committee, this concludes my prepared statement. I would be pleased to respond to any questions you and the Committee Members may have.

## Contact and Staff Acknowledgments

For further information about this statement, please contact William O. Jenkins Jr., Director, Homeland Security and Justice Issues, on (202) 512-8777 or jenkinswo@gao.gov.

Major contributors to this testimony included Chris Keisling, Assistant Director; John Vocino, Analyst-in-Charge; and Katherine Davis, Communications Analyst.

# Appendix I: Related GAO Products

*Homeland Security Grants: Observations on Process DHS Used to Allocate Funds to Selected Urban Areas*. GAO-07-381. Washington, D.C.: February 7, 2006.

*Homeland Security: Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks*. GAO-07-375. Washington, D.C.: January 24, 2007.

*Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*. GAO-07-225T. Washington, D.C.: January 18, 2007.

*Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program*. GAO-06-1090T. Washington, D.C.: September 7, 2006.

*Interagency Contracting: Improved Guidance, Planning, and Oversight Would Enable the Department of Homeland Security to Address Risks*. GAO-06-996. Washington, D.C.: September 27, 2006.

*Aviation Security: TSA Oversight of Checked Baggage Screening Procedures Could Be Strengthened*. GAO-06-869. Washington, D.C.: July 28, 2006.

*Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program*. GAO-06-854. Washington, D.C.: July 28, 2006.

*Passenger Rail Security: Evaluating Foreign Security Practices and Risk Can Help Guide Security Efforts*. GAO-06-557T. Washington, D.C.: March 29, 2006.

*Hurricane Katrina: GAO's Preliminary Observations Regarding Preparedness, Response, and Recovery*. GAO-06-442T. Washington, D.C.: March 8, 2006.

*Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*. GAO-06-91. Washington, D.C.: December 15, 2005.

*Strategic Budgeting: Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities*. GAO-05-824T. Washington, D.C.: June 29, 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. Washington, D.C.: February 15, 2005.

*Homeland Security: Observations on the National Strategies Related to Terrorism*. GAO-04-1075T. Washington, D.C.: September 22, 2004.

*9/11 Commission Report: Reorganization, Transformation, and Information Sharing*. GAO-04-1033T. Washington, D.C.: August 3, 2004.

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

Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System. GAO-04-682. Washington, D.C.: June 25, 2004.

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

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

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

*Homeland Security: Risk Communication Principles May Assist in Refinement of the Homeland Security Advisory System.* GAO-04-538T. Washington, D.C.: March 16, 2004.

*Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*. GAO-04-408T. Washington, D.C.: February 3, 2004.

*Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*. GAO-03-1165T. Washington, D.C.: September 17, 2003.

*Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*. GAO-03-760. Washington, D.C.: August 27, 2003.

*Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*. GAO-03-715T. Washington, D.C.: May 8, 2003.

*Transportation Security Research: Coordination Needed in Selecting and Implementing Infrastructure Vulnerability Assessments*. GAO-03-502. Washington, D.C.: May 1, 2003.

*Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*. GAO-03-322. Washington, D.C.: April 15, 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.

*Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*. GAO-03-233. Washington, D.C.: February 28, 2003.

*Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*. GAO-03-173. Washington, D.C.: January 30, 2003.

*Major Management Challenges and Program Risks: Department of Homeland Security*. GAO-03-103. Washington, D.C.: January 30, 2003.

*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.

*Homeland Security: A Framework for Addressing the Nation's Issues*. GAO-01-1158T. Washington, D.C.: September 21, 2001.

*Combating Terrorism: Selected Challenges and Related Recommendations*. GAO-01-822. Washington, D.C.: September 20, 2001.

*Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*. GAO-01-323. Washington, D.C.: April 25, 2001.

*Combating Terrorism: Linking Threats to Strategies and Resources*. GAO-00-218. Washington, D.C.: July 26, 2000.

*Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*. GAO-03-173. Washington, D.C.: April 9, 1998.

## 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