United States Government Accountability Office

GAO

Report to Congressional Requesters

August 2007

# DEPARTMENT OF HOMELAND SECURITY

## Progress Report on Implementation of Mission and Management Functions

GAO-07-454

GAO
Accountability·Integrity·Reliability

# Highlights

Highlights of GAO-07-454, a report to congressional requesters

## Why GAO Did This Study

The Department of Homeland Security's (DHS) recent 4 year anniversary provides an opportunity to reflect on the progress DHS has made since its establishment. DHS began operations in March 2003 with the mission to prevent terrorist attacks within the United States, reduce vulnerabilities, minimize damages from attacks, and aid in recovery efforts. GAO has reported that the creation of DHS was an enormous management challenge and that the size, complexity, and importance of the effort made the challenge especially daunting and critical to the nation's security. Our prior work on mergers and acquisitions found that successful transformations of large organizations, even those faced with less strenuous reorganizations than DHS, can take at least 5 to 7 years to achieve. GAO was asked to report on DHS's progress in implementing its mission and management areas and challenges DHS faces. This report also discusses key themes that have affected DHS's implementation efforts.

## How GAO Did This Study

To assess DHS's progress, GAO identified performance expectations for each mission and management area based on legislation, homeland security presidential directives, DHS and component agencies' strategic plans, and other sources.

(Continued on next page)

www.gao.gov/cgi-bin/getrpt?GAO-07-454.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Norman J. Rabkin at (202) 512-8777 or rabkinn@gao.gov.

August 17, 2007

# DEPARTMENT OF HOMELAND SECURITY

# Progress Report on Implementation of Mission and Management Functions

## What GAO Found

At the time of its creation in 2003 as one of the largest federal reorganizations in the last several decades, we designated the implementation and transformation of DHS as a high-risk area due to the magnitude of the challenges it confronted in areas vital to the physical and economic well being of the nation. After 4 years into its overall integration effort, DHS has attained some level of progress in all of its mission and management areas. The rate of progress, however, among these areas varies, as shown in the table below.

**Summary of Assessments of DHS's Progress in Mission and Management Areas**

| Mission/ management area | Number of performance expectations | Number of expectations generally achieved | Number of expectations generally not achieved | Number of expectations not assessed | Overall assessment of progress |
|---|---|---|---|---|---|
| Border security | 12 | 5 | 7 | 0 | Modest |
| Immigration enforcement | 16 | 8 | 4 | 4 | Moderate |
| Immigration services | 14 | 5 | 9 | 0 | Modest |
| Aviation security | 24 | 17 | 7 | 0 | Moderate |
| Surface transportation security | 5 | 3 | 2 | 0 | Moderate |
| Maritime security | 23 | 17 | 4 | 2 | Substantial |
| Emergency preparedness and response | 24 | 5 | 18 | 1 | Limited |
| Critical infrastructure protection | 7 | 4 | 3 | 0 | Moderate |
| Science and technology | 6 | 1 | 5 | 0 | Limited |
| Acquisition management | 3 | 1 | 2 | 0 | Modest |
| Financial management | 7 | 2 | 5 | 0 | Modest |
| Human capital management | 8 | 2 | 6 | 0 | Limited |
| Information technology management | 13 | 2 | 8 | 3 | Limited |
| Real property management | 9 | 6 | 3 | 0 | Moderate |
| **Total** | **171** | **78** | **83** | **10** | |

Source: GAO analysis.

Definitions:
**Substantial progress:** DHS has taken actions to generally achieve more than 75 percent of the identified performance expectations.
**Moderate progress:** DHS has taken actions to generally achieve more than 50 percent but 75 percent or less of the identified performance expectations.
**Modest progress:** DHS has taken actions to generally achieve more than 25 percent but 50 percent or less of the identified performance expectations.
**Limited progress**: DHS has taken actions to generally achieve 25 percent or less of the identified performance expectations.

GAO analyzed these documents to identify responsibilities for DHS and obtained and incorporated feedback from DHS officials on the performance expectations. On the basis of GAO's and the DHS Office of Inspector General's (IG) prior work and updated information provided by DHS, GAO determined the extent to which DHS has taken actions to generally achieve each performance expectation. An assessment of generally achieved indicates that DHS has taken actions to satisfy most elements of the expectation, and an assessment of generally not achieved indicates that DHS has not yet taken actions to satisfy most elements of the expectation. An assessment of generally not achieved may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated no assessment made. Our assessment of DHS's progress relative to each performance expectation is not meant to imply that DHS should have fully achieved the performance expectation by the end of its fourth year. On the basis of this analysis, GAO determined whether DHS has made limited, modest, moderate, or substantial progress in each mission and management area. The assessments of progress do not reflect, nor are they intended to reflect, the extent to which DHS's actions have made the nation more secure in each area.

Key underlying themes have affected DHS's implementation efforts, and will be essential for the department to address as it moves forward. These include management, risk management, information sharing, and partnerships and coordination. For example, while DHS has made progress in transforming its component agencies into a fully functioning department, it has not yet addressed key elements of the transformation process, such as developing a comprehensive strategy for agency transformation and ensuring that management systems and functions are integrated. This lack of a comprehensive strategy and integrated management systems and functions limits DHS's ability to carry out its homeland security responsibilities in an effective, risk-based way. DHS also has not yet fully adopted and applied a risk management approach in implementing its mission and management functions. Some DHS component agencies, such as the Transportation Security Administration and the Coast Guard, have taken steps to do so, but DHS has not yet taken sufficient actions to ensure that this approach is used departmentwide. In addition, DHS has taken steps to share information and coordinate with homeland security partners, but has faced difficulties in these partnership efforts, such as in ensuring that the private sector receives better information on potential threats.

Given DHS's dominant role in securing the homeland, it is critical that the department's mission and management programs are operating as efficiently and effectively as possible. DHS has had to undertake these responsibilities while also working to transform itself into a fully functioning cabinet department—a difficult task for any organization. As DHS moves forward, it will be important for the department to continue to develop more measurable goals to guide implementation efforts and to enable better accountability of its progress toward achieving desired outcomes. It will also be important for DHS to continually reassess its mission and management goals, measures, and milestones to evaluate progress made, identify past and emerging obstacles, and examine alternatives to address those obstacles and effectively implement its missions.

## What GAO Recommends

While this report contains no new recommendations, in past products, GAO has made approximately 700 recommendations to DHS designed to strengthen departmental operations. DHS has implemented some of these recommendations, has taken actions to address others, and has taken other steps to strengthen its mission and management activities.

In its comments on a draft of this report, DHS took issues with our methodology and disagreed with our assessments for 42 of 171 performance expectations. DHS's five general concerns were with (1) perceived alteration of standards used to judge progress; (2) our binary approach to assess the performance expectations; (3) perceived changes in criteria after DHS provided additional information; (4) consistent application of our methodology; and (5) differences in the priority of performance expectations. We believe that we have fully disclosed and consistently applied our methodology and that it provides a sound basis for this progress report.

# Contents

**Tables**

## Figures

## Abbreviations

| | |
|---|---|
| CBP | U.S. Customs and Border Protection |
| DHS | Department of Homeland Security |
| DNDO | Domestic Nuclear Detection Office |
| EDS | explosive detection system |
| ETD | explosive trace detection |
| FEMA | Federal Emergency Management Agency |
| GPRA | Government Performance and Results Act |
| ICE | U.S. Immigration and Customs Enforcement |
| IG | Inspector General |
| INS | U.S. Immigration and Naturalization Service |
| OMB | Office of Management and Budget |
| SBI | Secure Border Initiative |
| TSA | Transportation Security Administration |
| USCIS | U.S. Citizenship and Immigration Services |
| US-VISIT | United States Visitor and Immigrant Status Indicator Technology |

G A O
Accountability * Integrity * Reliability

**United States Government Accountability Office**
**Washington, DC 20548**

August 17, 2007

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Department of Homeland Security (DHS) recently passed its 4 year anniversary, and this anniversary provides an opportunity to reflect on the progress it has made since its establishment, determine challenges the department has faced in implementing its mission and management areas, and identify issues that will be important for the department to address as it moves forward. Pursuant to the Homeland Security Act of 2002, DHS began operations in March 2003 with missions that include preventing terrorist attacks from occurring within the United States, reducing U.S. vulnerability to terrorism, minimizing the damages from attacks that occur, and helping the nation recover from any attacks. Over the past 4 years, the department has initiated and continued the implementation of various policies and programs to address these missions as well as its nonhomeland security functions.[1] In particular, DHS has implemented programs to secure the border and administer the immigration system; strengthen the security of the transportation sector; and defend against, prepare for, and respond to threats and disasters. DHS has also taken actions to integrate its management functions and to transform its component agencies into an effective cabinet department.

We have evaluated many of DHS's programs and management functions since the department's establishment. We have issued over 400 products on major departmental programs in the areas of border security and

[1] Examples of nonhomeland security functions include Coast Guard search and rescue and naturalization services.

immigration; transportation security; defense against, preparedness for, and response to threats and disasters; and the department's management functions—including acquisition, financial, human capital, information technology, and real property management. In November 2006, we provided congressional leadership with a list of government programs, functions, and activities that warrant further congressional oversight. Among the issues included were border security and immigration enforcement, security of transportation modes, preparedness and response for catastrophic threats, and DHS implementation and transformation.[2] We have also reported on broad themes that have underpinned DHS's implementation efforts, including agency transformation, strategic planning and results management, risk management, information sharing, and partnerships and coordination. We have made about 700 recommendations to DHS on ways to improve its operations and address these key themes, such as to develop performance measures and set milestones for key programs, allocate resources based on assessments of risk, and develop and implement internal controls to help ensure program effectiveness. DHS has implemented some of these recommendations, taken actions to address others, and taken other steps to strengthen its mission activities and facilitate management integration. However, we have reported that the department still has much to do to ensure that it conducts its missions efficiently and effectively while simultaneously preparing to address future challenges that face the department and the nation.

In 2003, we designated the implementation and transformation of DHS as high-risk because it represented an enormous undertaking that would require time to achieve in an effective and efficient manner.[3] Additionally, the components merged into DHS already faced a wide array of existing challenges, and any DHS failure to effectively carry out its mission could expose the nation to potentially serious consequences. The area has remained on our high-risk list since 2003.[4] Most recently, in our January 2007 high-risk update, we reported that although the department had made some progress transforming its 22 agencies into an effective, integrated organization, DHS had not yet developed a comprehensive management

[2] GAO, *Suggested Areas for Oversight for the 110th Congress*, GAO-07-235R (Washington, D.C.: Nov. 17, 2006).

[3] GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

[4] GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005) and GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

integration strategy and its management systems and functions—especially related to acquisition, financial, human capital, and information management—were not yet fully integrated and wholly operational. We also noted that DHS faces a number of challenges to effectively carry out its program activities and enhance partnerships with private and public sector entities to leverage resources. We concluded that this array of management and programmatic challenges continues to limit DHS's ability to fulfill its homeland security roles in an effective, risk-based way. Furthermore, in 2005 we designated information sharing for homeland security as high-risk,[5] and in 2006 we identified the National Flood Insurance Program as high-risk.[6] In 2003 we expanded the scope of the high-risk area involving federal information security, which was initially designated as high-risk in 1997, to include the protection of the nation's computer-reliant critical infrastructure. We identified information sharing for homeland security as high-risk because of the lack of strategic plans; established processes, procedures, and mechanisms; and incentives for sharing information. We identified the National Flood Insurance Program as high-risk because it was highly unlikely that the program would generate sufficient revenues to repay funds borrowed from the Treasury to cover claims during catastrophic loss years and because of concerns related to the program's financial resources, compliance with mandatory purchase requirements, and the costly impact of repetitive loss properties. We expanded the scope of the federal information security high-risk area to include the protection of the nation's computer-reliant critical infrastructure because, as the focal point of federal efforts, DHS had not yet completely fulfilled any of its key responsibilities for enhancing cyber security.

In designating the implementation and transformation of DHS as high-risk, we noted that the creation of DHS was an enormous management challenge.[7] The size, complexity, and importance of the effort made the challenge especially daunting and incomparably critical to the nation's security. We noted that building an effective department would require consistent and sustained leadership from top management to ensure the needed transformation of disparate agencies, programs, and missions into

[5] GAO-05-207 and GAO-07-310.

[6] GAO, *GAO's High-Risk Program*, GAO-06-497T (Washington, D.C.: Mar. 15, 2006) and GAO-07-310.

[7] GAO, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: January 2003).

an integrated organization. Our prior work on mergers and acquisitions, undertaken before the creation of DHS, found that successful transformations of large organizations, even those faced with less strenuous reorganizations than DHS, can take 5 to 7 years to achieve. We reported that in successful transformations, organizations undergo a change of their cultures to become more results-oriented, client- and customer-oriented, and collaborative in nature. To successfully transform, an organization must fundamentally reexamine its processes, organizational structures, and management approaches. Organizational changes such as these are complex and cannot be accomplished overnight. In the case of DHS, it will likely take at least several more years for the department to complete its transformation efforts. We also have recommended that Congress continue to monitor whether it needs to provide additional leadership authorities to the DHS Under Secretary for Management or create a Chief Operating Officer/Chief Management Officer position that could help elevate, integrate, and institutionalize DHS's management initiatives. The Implementing Recommendations of the 9/11 Commission Act of 2007, enacted in August 2007, designates the Under Secretary for Management as the Chief Management Officer and principal advisor on management-related matters to the Secretary.[8] Under the Act, the Under Secretary is responsible for developing a transition and succession plan for the incoming Secretary and Under Secretary to guide the transition of management functions to a new administration. The Act further authorizes the incumbent Under Secretary as of November 8, 2008 (after the next presidential election), to remain in the position until a successor is confirmed to ensure continuity in the management functions of DHS.

You asked us to review our past work on DHS and provide an assessment of DHS's progress and challenges during its first 4 years. This report addresses the following questions: (1) What progress has DHS made in implementing key mission and core management functions since its inception, and what challenges has the department faced in its implementation efforts? (2) What key themes have affected DHS's implementation of its mission and management functions?[9]

[8] Implemented Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 2405, 121 Stat. 266 (2007).

[9] This report also addresses our mandate at section 477(d)(2) of the Homeland Security Act of 2002. Pub. L. No. 107-296, 116 Stat. 2135, 2210-11.

DHS's major mission and management areas include border security; immigration enforcement; immigration services; aviation security; surface transportation security; maritime security; emergency preparedness and response; critical infrastructure and key resources protection; science and technology; and acquisition, financial, human capital, information technology, and real property management. This report also identifies the key cross-cutting themes that have affected the department's efforts to implement its mission and management areas. These key themes include agency transformation, strategic planning and results management, risk management, information sharing, and partnerships and coordination.

## Scope and Methodology

This report is based primarily on work that we and the DHS Office of Inspector General (IG) have completed since the establishment of DHS in March 2003 and updated information and documentation provided by the department in March 2007 through July 2007. To determine the progress DHS has made in implementing various mission and management areas, we first identified key areas. To identify these mission and management areas, we analyzed the critical mission areas for homeland security identified in legislation, the *National Strategy for Homeland Security*, the goals and objectives set forth in the DHS Strategic Plan and homeland security presidential directives, and areas identified in our reports along with studies conducted by the DHS IG and other organizations and groups, such as the National Commission on Terrorist Attacks upon the United States (9-11 Commission) and the Century Foundation. We analyzed these documents to identify common mission and management areas and discussed the areas we identified with our subject matter experts[10] and DHS officials.[11] The mission and management areas we identified are:

1. Border security

[10] Our subject matter experts are individuals within GAO who have directed and managed work related to the DHS mission and management areas.

[11] We focused these mission areas primarily on DHS's homeland security-related functions. We did not consider the Secret Service, domestic counterterrorism, intelligence activities, or trade enforcement functions because (1) GAO and the DHS Office of Inspector General have completed limited work in these areas; (2) there are few, if any, requirements identified for the Secret Service's mission and for DHS's role in domestic counterterrorism and intelligence (the Department of Justice serves as the lead agency for most counterterrorism initiatives); and (3) we address DHS actions that could be considered part of domestic counterterrorism and intelligence in other areas, such as aviation security, critical infrastructure and key resources protection, and border security.

2. Immigration enforcement

3. Immigration services

4. Aviation security

5. Surface transportation security

6. Maritime security

7. Emergency preparedness and response

8. Critical infrastructure and key resources protection

9. Science and technology

10. Acquisition management

11. Financial management

12. Human capital management

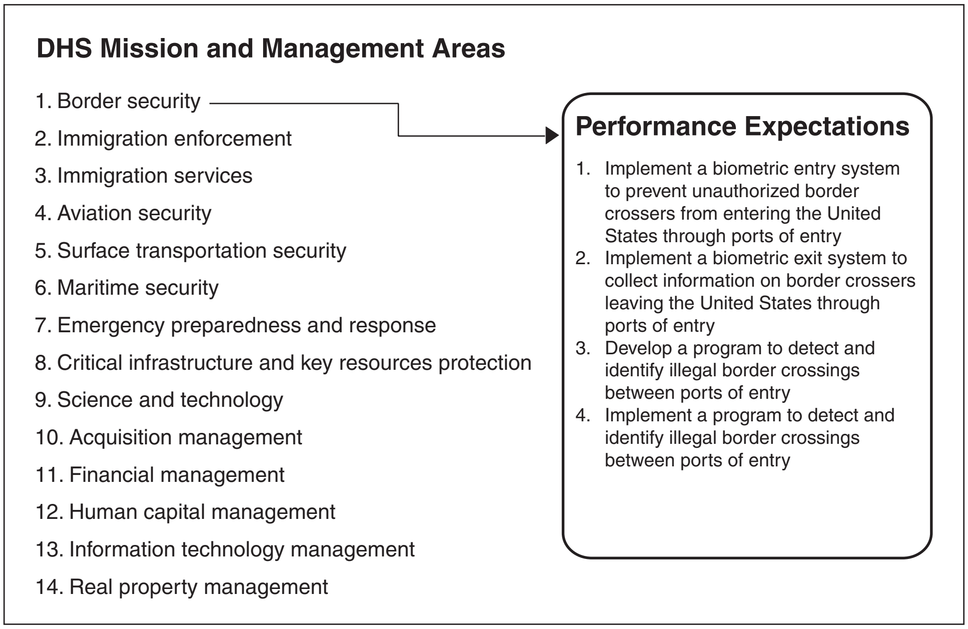
13. Information technology management

14. Real property management

To determine the level of progress made by DHS in each mission and management area, we identified performance expectations for each area. We define performance expectations as a composite of the responsibilities or functions—derived from legislation, homeland security presidential directives and executive orders, DHS planning documents, and other sources—that the department is to achieve or satisfy in implementing efforts in its mission and management areas. The performance expectations are not intended to represent performance goals or measures for the department.[12] Figure 1 provides an example of performance expectations for the border security mission area:

[12] A performance goal is the target level of performance expressed as a tangible, measurable objective against which actual achievement will be compared. A performance measure can be defined as an indicator, statistic, or metric used to gauge program performance.

**Figure 1: Example of Performance Expectations for Border Security**



DHS Mission and Management Areas

1. Border security
2. Immigration enforcement
3. Immigration services
4. Aviation security
5. Surface transportation security
6. Maritime security
7. Emergency preparedness and response
8. Critical infrastructure and key resources protection
9. Science and technology
10. Acquisition management
11. Financial management
12. Human capital management
13. Information technology management
14. Real property management

Performance Expectations

1. Implement a biometric entry system to prevent unauthorized border crossers from entering the United States through ports of entry
2. Implement a biometric exit system to collect information on border crossers leaving the United States through ports of entry
3. Develop a program to detect and identify illegal border crossings between ports of entry
4. Implement a program to detect and identify illegal border crossings between ports of entry

Source: GAO.

We primarily focused the performance expectations on DHS's homeland security-related functions. We generally did not identify performance expectations related to DHS's nonhomeland security functions, although we did identify some performance expectations that relate to these functions. We also did not apply a weight to the performance expectations we developed for DHS, although qualitative differences between the expectations exist. We recognize that these expectations are not time bound, and DHS will take actions to satisfy these expectations over a sustained period of time. Therefore, our assessment of DHS's progress relative to each performance expectation refers to the progress made by the department during its first 4 years. Our assessment of DHS's progress relative to each performance expectation is not meant to imply that DHS should have fully achieved the performance expectation by the end of its fourth year.

To identify the performance expectations, we examined responsibilities set for the department by Congress, the Administration, and department leadership. In doing so, we reviewed homeland security-related legislation, such as the Intelligence Reform and Terrorism Prevention Act of 2004,[13] the Homeland Security Act of 2002,[14] the Maritime Transportation Security Act of 2002,[15] the Enhanced Border Security and Visa Entry Reform Act of 2002,[16] and the Aviation and Transportation Security Act.[17] We also reviewed DHS appropriations acts and accompanying conference reports for fiscal years 2004 through 2006. We did not consider legislation enacted since September 2006 in developing the performance expectations. To identify goals and measures set by the Administration, we reviewed relevant homeland security presidential directives and executive orders. For the goals and measures set by the department, we analyzed the DHS Strategic Plan, Performance Budget Overviews, Performance and Accountability Reports, and component agencies' strategic plans. For management areas, we also examined effective practices identified in our

[13] Pub. L. No. 108-458, 118 Stat. 3638 (2004).

[14] Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[15] Pub. L. No. 107-295, 116 Stat. 2064 (2002).

[16] Pub. L. No. 107-173, 116 Stat. 543 (2002).

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

prior reports.[18] We analyzed these documents to identify common or similar responsibilities for DHS mission and management areas and synthesized the responsibilities identified in the various documents to develop performance expectations for DHS. We obtained and incorporated feedback from our subject matter experts on these performance expectations. We also provided the performance expectations to DHS for review and incorporated DHS's feedback.

Based primarily on our prior work and DHS IG work, as well as updated information provided by DHS between March and June 2007, we examined the extent to which DHS has taken actions to achieve the identified performance expectations in each area and make a determination as to whether DHS has achieved the key elements of each performance expectation based on the criteria listed below:

- **Generally achieved:** Our work has shown that DHS has taken actions to satisfy most of the key elements of the performance expectation but may not have satisfied all of the elements.

[18] We reviewed various effective practices reports for each management area. For acquisition management, we reviewed GAO, *Best Practices: Taking a Strategic Approach Could Improve DOD's Acquisition of Services*, GAO-02-230 (Washington, D.C.: Jan. 18, 2002); GAO, *2010 Census: Census Bureau Generally Follows Selected Leading Acquisition Planning Practices, but Continued Management Attention Is Needed to Help Ensure Success*, GAO-06-277 (Washington, D.C.: May 18, 2006); and GAO, *A Framework for Assessing the Acquisition Function at Federal Agencies*, GAO-05-218G (Washington, D.C.: September 2005). For financial management, we reviewed GAO, *Financial Management Systems: DHS Has an Opportunity to Incorporate Best Practices in Modernization Efforts*, GAO-06-553T (Washington, D.C.: Mar. 29, 2006). For human capital, we reviewed GAO, *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: Mar. 15, 2002); GAO, *Managing for Results: Using Strategic Human Capital Management to Drive Transformational Change*, GAO-02-940T (Washington, D.C.: July 15, 2002); GAO, *Human Capital: A Self-Assessment Checklist for Agency Leaders*, GAO/OCG-00-14G (Washington, D.C: September 2000); and GAO, *Department of Homeland Security: Strategic Management of Training Important for Successful Transformation*, GAO-05-888 (Washington, D.C.: Sept. 23, 2005). For information technology, we reviewed GAO, *Homeland Security: Progress Continues, but Challenges Remain on Department's Management of Information Technology*, GAO-06-598T (Washington, D.C.: Mar. 29, 2006); GAO, *Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation*, GAO-06-831 (Washington, D.C.: Aug. 14, 2006); GAO, *Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach*, GAO-04-702 (Washington, D.C.: Aug. 27, 2004); GAO, *Maximizing the Success of Chief Information Officers*, GAO-01-376G (Washington, D.C.: February 2001); and GAO, *Improving Mission Performance through Strategic Information Management and Technology*, GAO/AIMD-94-115 (Washington, D.C.: May 1994).

- **Generally not achieved:** Our work has shown that DHS has not yet taken actions to satisfy most of the key elements of the performance expectation but may have taken steps to satisfy some of the elements.

- **No assessment made:** Neither we nor the DHS IG have completed work and/or the information DHS provided did not enable us to clearly assess DHS's progress in achieving the performance expectation. Therefore, we have no basis for making an assessment of the extent to which DHS has taken actions to satisfy the performance expectation.[19]

An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation; however, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made." We analyzed the extent of our work, the DHS IG's work, and DHS's updated information and conferred with our subject matter experts to determine whether the work and information were sufficient for a making a determination of generally achieved or generally not achieved.

Between March and June 2007, we obtained updated information from DHS and met with program officials to discuss DHS's efforts to implement actions to achieve the performance expectations in each mission and management area. We incorporated DHS's additional information and documentation into the report and, to the extent that DHS provided

[19] These assessments of "generally achieved," "generally not achieved," and "no assessment made" apply to the performance expectations we identified for DHS in each mission and management area. For example, as shown in figure 1, they apply to the performance expectations we identified for the border security mission area, such as "implement a biometric entry system to prevent unauthorized border crossers from entering the United States through ports of entry." They do not apply to DHS mission and management areas, such as border security or immigration enforcement.

documentation verifying its efforts, considered them in making our assessments of DHS's progress.

For each performance expectation, an analyst on our staff reviewed our relevant work, DHS IG reports, and updated information and documentation provided by DHS, including information received during meetings with DHS officials. On the basis of this review, the analyst made a determination that either DHS generally achieved the performance expectation or generally did not achieve the performance expectation, or the analyst identified that no determination could be made because neither we nor the DHS IG had completed work and DHS did not provide us with updated information and documentation. A second analyst then reviewed each determination to reach concurrence on the assessment for each performance expectation by reviewing the first analyst's summary of our reports, relevant DHS IG reports, and DHS's updated information and documentation. In cases when the first and second analyst disagreed, the two analysts reviewed and discussed the assessments and relevant documents to reach concurrence. Then, our subject matter experts reviewed the summary of our reports, relevant DHS IG reports, and DHS's updated information and documentation to reach concurrence on the assessment for each performance expectation.

To develop criteria for assessing DHS's progress in each mission and management area, we analyzed criteria used for ratings or assessments in our prior work, in DHS IG reports, and in other reports and studies, such as those conducted by the 9-11 Commission and the Century Foundation. We also reviewed our past work in each mission and management area and obtained feedback from our subject matter experts and DHS officials on these criteria. Based on this analysis, we developed the following criteria for assessing DHS's progress in each mission and management area:

- **Substantial progress:** DHS has taken actions to generally achieve more than 75 percent of the identified performance expectations.
- **Moderate progress:** DHS has taken actions to generally achieve more than 50 percent but 75 percent or less of the identified performance expectations.
- **Modest progress:** DHS has taken actions to generally achieve more than 25 percent but 50 percent or less of the identified performance expectations.
- **Limited progress**: DHS has taken actions to generally achieve 25 percent or less of the identified performance expectations.

After making a determination as to whether DHS has generally achieved or generally not achieved the identified performance expectations, we added up the number of performance expectations that we determined DHS has generally achieved. We divided this number by the total number of performance expectations for each mission and management area, excluding those performance expectations for which we could not make an assessment. Based on the resulting percentage, we identified DHS's overall progress in each mission and management area, as (1) substantial progress, (2) moderate progress, (3) modest progress, or (4) limited progress. Our subject matter experts reviewed the overall assessments of progress we identified for DHS in each mission and management area.

Our assessments of the progress made by DHS in each mission and management area are based on the performance expectations we identified. The assessments of progress do not reflect, nor are they intended to reflect, the extent to which DHS's actions have made the nation more secure in each area. For example, in determining that DHS has made modest progress in border security, we are not stating or implying that the border is modestly more secure than it was prior to the creation of DHS. In addition, we are not assessing DHS's progress against a baseline in each mission and management area. We also did not consider DHS component agencies' funding levels or the extent to which funding levels have affected the department's ability to carry out its missions. We also did not consider the extent to which competing priorities and resource demands have affected DHS's progress in each mission and management area relative to other areas, although competing priorities and resource demands have clearly affected DHS's progress in specific areas.

In addition, because we and the DHS IG have completed varying degrees of work (in terms of the amount and scope of reviews completed) for each mission and management area, and because different DHS components and offices provided us with different amounts and types of information, our assessments of DHS's progress in each mission and management area reflect the information available for our review and analysis and are not necessarily equally comprehensive across all 14 mission and management areas. For example, as a result of the post-September 11, 2001, focus on aviation, we have conducted more reviews of aviation security, and our methodology identified a much larger number of related performance expectations than for the department's progress in surface transportation security. Further, for some performance expectations, we were unable to make an assessment of DHS's progress because (1) we had not conducted work in that area, (2) the DHS IG's work in the area was also limited, and

(3) the supplemental information provided by DHS was insufficient to form a basis for our analysis. Most notably, we were unable to make an assessment for four performance expectations in the area of immigration enforcement. This affected our overall assessment of DHS's progress in that area as there were fewer performance expectations to tally in determining the overall level of progress.

We conducted our work for this report from September 2006 through July 2007 in accordance with generally accepted government auditing standards.

## Results in Brief

At the time of its creation in 2003 as one of the largest federal reorganizations in the last several decades, we designated the implementation and transformation of DHS as a high-risk area due to the magnitude of the challenges it confronted in areas vital to the physical and economic well being of the nation. After 4 years into its overall integration effort, DHS has attained some level of progress in all of its major mission and management areas. The rate of progress, however, among these areas varies.

- DHS's **border security** mission includes detecting and preventing terrorists and terrorist weapons from entering the United States; facilitating the orderly and efficient flow of legitimate trade and travel; interdicting illegal drugs and other contraband; apprehending individuals who are attempting to enter the United States illegally; inspecting inbound and outbound people, vehicles, and cargo; and enforcing pertinent laws of the United States at the border. As shown in table 1, we identified 12 performance expectations for DHS in the area of border security and found that DHS has generally achieved 5 of them and has generally not achieved 7 others.

Table 1: Summary of Our Assessments for DHS's Border Security Performance Expectations

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **5** |
| Implement a biometric entry system to prevent unauthorized border crossers from entering the United States through ports of entry | |
| Develop a program to detect and identify illegal border crossings between ports of entry | |
| Develop a strategy to detect and interdict illegal flows of cargo, drugs, and other items into the United States | |
| Provide adequate training for all border related employees | |
| Develop staffing plans for hiring and allocating human capital resources to fulfill the agency's border security mission | |
| **Generally not achieved** | **7** |
| Implement a biometric exit system to collect information on border crossers leaving the United States through ports of entry | |
| Implement a program to detect and identify illegal border crossings between ports of entry | |
| Implement a strategy to detect and interdict illegal flows of cargo, drugs and other items into the United States | |
| Implement effective security measures in the visa issuance process | |
| Implement initiatives related to the security of certain documents used to enter the United States | |
| Ensure adequate infrastructure and facilities | |
| Leverage technology, personnel, and information to secure the border | |
| **Overall assessment of progress** | **Modest** |

Source: GAO analysis.

- DHS's **immigration enforcement** mission includes apprehending, detaining, and removing criminal and illegal aliens; disrupting and dismantling organized smuggling of humans and contraband as well as human trafficking; investigating and prosecuting those who engage in benefit and document fraud; blocking and removing employers' access to undocumented workers; and enforcing compliance with programs to monitor visitors. As shown in table 2, we identified 16 performance expectations for DHS in the area of immigration enforcement and found that DHS has generally achieved 8 of them and has generally not achieved 4 others. For 4 performance expectations, we could not make an assessment.

Table 2: Summary of Our Assessments for DHS's Immigration Enforcement Performance Expectations

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **8** |
| Develop a program to ensure the timely identification and removal of noncriminal aliens subject to removal from the United States | |
| Assess and prioritize the use of alien detention resources to prevent the release of aliens subject to removal | |
| Develop a program to allow for the secure alternative detention of noncriminal aliens | |
| Develop a prioritized worksite enforcement strategy to ensure that only authorized workers are employed | |
| Develop a comprehensive strategy to interdict and prevent trafficking and smuggling of aliens into the United States | |
| Develop a law enforcement strategy to combat criminal alien gangs in the United States and cross-border criminal activity | |
| Develop a program to screen and respond to local law enforcement and community complaints about aliens who many be subject to removal | |
| Develop staffing plans for hiring and allocating human capital resources to fulfill the agency's immigration enforcement mission | |
| **Generally not achieved** | **4** |
| Implement a program to ensure the timely identification and removal of noncriminal aliens subject to removal from the United States | |
| Ensure the removal of criminal aliens | |
| Implement a prioritized worksite enforcement strategy to ensure that only authorized workers are employed | |
| Implement a comprehensive strategy to interdict and prevent trafficking and smuggling of aliens into the United States | |
| **No assessment made** | **4** |
| Implement a program to allow for the secure alternative detention of noncriminal aliens | |
| Implement a law enforcement strategy to combat criminal alien gangs in the United States and cross-border criminal activity | |
| Disrupt and dismantle mechanisms for money laundering and financial crimes | |
| Provide training, including foreign language training, and equipment for all immigration enforcement personnel to fulfill the agency's mission | |
| **Overall assessment of progress** | **Moderate** |

Source: GAO analysis.

- DHS's **immigration services** mission includes administering immigration benefits and working to reduce immigration benefit fraud. As shown in table 3, we identified 14 performance expectations for

DHS in the area of immigration services and found that DHS has generally achieved 5 of them and has generally not achieved 9 others.

**Table 3: Summary of Our Assessments for DHS's Immigration Services Performance Expectations**

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **5** |
| Institute process and staffing reforms to improve application processes | |
| Establish online access to status information about benefit applications | |
| Establish revised immigration application fees based on a comprehensive fee study | |
| Communicate immigration-related information to other relevant agencies | |
| Create an office to reduce immigration benefit fraud | |
| **Generally not achieved** | **9** |
| Eliminate the benefit application backlog and reduce application completion times to 6 months | |
| Establish a timetable for reviewing the program rules, business processes, and procedures for immigration benefit applications | |
| Institute a case management system to manage applications and provide management information | |
| Develop new programs to prevent future backlogs from developing | |
| Establish online filing for benefit applications | |
| Capture biometric information on all benefits applicants | |
| Implement an automated background check system to track and store all requests for applications | |
| Establish training programs to reduce fraud in the benefits process | |
| Implement a fraud assessment program to reduce benefit fraud | |
| **Overall assessment of progress** | **Modest** |

Source: GAO analysis.

- DHS's **aviation security** mission includes strengthening airport security; providing and training a screening workforce; prescreening passengers against terrorist watch lists; and screening passengers, baggage, and cargo. As shown in table 4, we identified 24 performance expectations for DHS in the area of aviation security and found that DHS has generally achieved 17 of them and has generally not achieved 7 others.

Table 4: Summary of Our Assessments for DHS's Aviation Security Performance Expectations

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **17** |
| Implement a strategic approach for aviation security functions | |
| Ensure the screening of airport employees against terrorist watch lists | |
| Hire and deploy a federal screening workforce | |
| Develop standards for determining aviation security staffing at airports | |
| Establish standards for training and testing the performance of airport screener staff | |
| Establish a program and requirements to allow eligible airports to use a private screening workforce | |
| Train and deploy federal air marshals on high-risk flights | |
| Establish standards for training flight and cabin crews | |
| Establish a program to allow authorized flight deck officers to use firearms to defend against any terrorist or criminal acts | |
| Establish policies and procedures to ensure that individuals known to pose, or suspected of posing, a risk or threat to security are identified and subjected to appropriate action | |
| Develop and implement processes and procedures for physically screening passengers at airport checkpoints | |
| Develop and test checkpoint technologies to address vulnerabilities | |
| Deploy explosive detection systems (EDS) and explosive trace detection (ETD) systems to screen checked baggage for explosives | |
| Develop a plan to deploy in-line baggage screening equipment at airports | |
| Pursue the deployment and use of in-line baggage screening equipment at airports | |
| Develop a plan for air cargo security | |
| Develop and implement procedures to screen air cargo | |

| Performance expectation | Total |
|---|---|
| **Generally not achieved** | **7** |
| Establish standards and procedures for effective airport perimeter security | |
| Establish standards and procedures to effectively control access to airport secured areas | |
| Establish procedures for implementing biometric identifier systems for airport secured areas access control | |
| Develop and implement an advanced prescreening system to allow DHS to compare domestic passenger information to the Selectee List and No Fly List | |
| Develop and implement an international passenger prescreening process to compare passenger information to terrorist watch lists before aircraft departure | |
| Deploy checkpoint technologies to address vulnerabilities | |
| Develop and implement technologies to screen air cargo | |
| **Overall assessment of progress** | **Moderate** |

Source: GAO analysis.

- DHS's **surface transportation security** mission includes establishing security standards and conducting assessments and inspections of surface transportation modes, which include passenger and freight rail; mass transit; highways, including commercial vehicles; and pipelines. As shown in table 5, we identified 5 performance expectations for DHS in the area of surface transportation security and found that DHS has generally achieved 3 of them and has generally not achieved 2.

**Table 5: Summary of Our Assessments for DHS's Surface Transportation Security Performance Expectations**

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **3** |
| Develop and adopt a strategic approach for implementing surface transportation security functions | |
| Conduct threat, criticality, and vulnerability assessments of surface transportation assets | |
| Administer grant programs for surface transportation security | |
| **Generally not achieved** | **2** |
| Issue standards for securing surface transportation modes | |
| Conduct compliance inspections for surface transportation systems | |
| **Overall assessment of progress** | **Moderate** |

Source: GAO analysis.

- DHS's **maritime security** responsibilities include port and vessel security, maritime intelligence, and maritime supply chain security. As shown in table 6, we identified 23 performance expectations for DHS in the area of maritime security and found that DHS has generally achieved 17 of them and has generally not achieved 4 others. For 2 performance expectations, we could not make an assessment.

**Table 6: Summary of Our Assessments for DHS's Maritime Security Performance Expectations**

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **17** |
| Develop national plans for maritime security | |
| Develop national plans for maritime response | |
| Develop national plans for maritime recovery | |
| Develop regional (port-specific) plans for security | |
| Develop regional (port-specific) plans for response | |
| Ensure port facilities have completed vulnerability assessments and developed security plans | |
| Ensure that vessels have completed vulnerability assessments and developed security plans | |
| Exercise security, response, and recovery plans with key maritime stakeholders to enhance security, response, and recovery efforts | |
| Implement a port security grant program to help facilities improve their security capabilities | |
| Establish operational centers to monitor threats and fuse intelligence and operations at the regional/port level | |
| Collect information on incoming ships to assess risks and threats | |
| Develop a vessel-tracking system to improve intelligence and maritime domain awareness on vessels in U.S. waters | |
| Collect information on arriving cargo for screening purposes | |
| Develop a system for screening and inspecting cargo for illegal contraband | |
| Develop a program to work with foreign governments to inspect suspicious cargo before it leaves for U.S. ports | |
| Develop a program to work with the private sector to improve and validate supply chain security | |
| Develop an international port security program to assess security at foreign ports | |
| **Generally not achieved** | **4** |
| Develop regional (port-specific) plans for recovery | |
| Implement a national facility access control system for port secured areas | |

| Performance expectation | Total |
|---|---|
| Develop a long-range vessel-tracking system to improve maritime domain awareness | |
| Develop a program to screen incoming cargo for radiation | |
| **No assessment made** | **2** |
| Develop a national plan to establish and improve maritime intelligence | |
| Develop standards for cargo containers to ensure their physical security | |
| **Overall assessment of progress** | **Substantial** |

Source: GAO analysis.

- DHS's **emergency preparedness and response** mission includes preparing to minimize the damage and recover from terrorist attacks and disasters; helping to plan, equip, train, and practice needed skills of first responders; and consolidating federal response plans and activities to build a national, coordinated system for incident management. As shown in table 7, we identified 24 performance expectations for DHS in the area of emergency preparedness and response and found that DHS has generally achieved 5 of them and has generally not achieved 18 others. For 1 performance expectation, we could not make an assessment.

**Table 7: Summary of Our Assessments for DHS's Emergency Preparedness and Response Performance Expectations**

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **5** |
| Establish a program for conducting emergency preparedness exercises | |
| Develop a national incident management system | |
| Provide grant funding to first responders in developing and implementing interoperable communications capabilities | |
| Administer a program for providing grants and assistance to state and local governments and first responders | |
| Allocate grants based on assessment factors that account for population, critical infrastructure, and other risk factors | |
| **Generally not achieved** | **18** |
| Establish a comprehensive training program for national preparedness | |
| Conduct and support risk assessments and risk management capabilities for emergency preparedness | |
| Ensure the capacity and readiness of disaster response teams | |
| Coordinate implementation of a national incident management system | |
| Establish a single, all-hazards national response plan | |

| Performance expectation | Total |
|---|---|
| Coordinate implementation of a single, all-hazards response plan | |
| Develop a complete inventory of federal response capabilities | |
| Develop a national, all-hazards preparedness goal | |
| Develop plans and capabilities to strengthen nationwide recovery efforts | |
| Develop the capacity to provide needed emergency assistance and services in a timely manner | |
| Provide timely assistance and services to individuals and communities in response to emergency events | |
| Implement a program to improve interoperable communications among federal, state, and local agencies | |
| Implement procedures and capabilities for effective interoperable communications | |
| Increase the development and adoption of interoperability communications standards | |
| Develop performance goals and measures to assess progress in developing interoperability | |
| Provide guidance and technical assistance to first responders in developing and implementing interoperable communications capabilities | |
| Provide assistance to state and local governments to develop all-hazards plans and capabilities | |
| Develop a system for collecting and disseminating lessons learned and best practices to emergency responders | |
| **No assessment made** | **1** |
| Support citizen participation in national preparedness efforts | |
| **Overall assessment of progress** | **Limited** |

Source: GAO analysis.

- DHS's **critical infrastructure and key resources protection** activities include developing and coordinating implementation of a comprehensive national plan for critical infrastructure protection, developing partnerships with stakeholders and information sharing and warning capabilities, and identifying and reducing threats and vulnerabilities. As shown in table 8, we identified 7 performance expectations for DHS in the area of critical infrastructure and key resources protection and found that DHS has generally achieved 4 of them and has generally not achieved 3 others.

Table 8: Summary of Our Assessments for DHS's Critical Infrastructure and Key Resources Protection Performance Expectations

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **4** |
| Develop a comprehensive national plan for critical infrastructure protection | |
| Develop partnerships and coordinate with other federal agencies, state and local, governments, and the private sector | |
| Identify and assess threats and vulnerabilities for critical infrastructure | |
| Support efforts to reduce threats and vulnerabilities for critical infrastructure | |
| **Generally not achieved** | **3** |
| Improve and enhance public/private information sharing involving attacks, threats, and vulnerabilities | |
| Develop and enhance national analysis and warning capabilities for critical infrastructure | |
| Provide and coordinate incident response and recovery planning efforts for critical infrastructure | |
| **Overall assessment of progress** | **Moderate** |

Source: GAO analysis.

- DHS's **science and technology** efforts include coordinating the federal government's civilian efforts to identify and develop countermeasures to chemical, biological, radiological, nuclear, and other emerging terrorist threats. As shown in table 9, we identified 6 performance expectations for DHS in the area of science and technology and found that DHS has generally achieved 1 of them and has generally not achieved 5 others.

Table 9: Summary of Our Assessments for DHS's Science and Technology Performance Expectations

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **1** |
| Coordinate with and share homeland security technologies with federal, state, local, and private sector entities | |
| **Generally not achieved** | **5** |
| Develop a plan for departmental research, development, testing, and evaluation activities | |
| Assess emerging chemical, biological, radiological, and nuclear threats and homeland security vulnerabilities | |
| Coordinate research, development, and testing efforts to identify and develop countermeasures to address chemical, biological, radiological, nuclear, and other emerging terrorist threats | |
| Coordinate deployment of nuclear, biological, chemical, and radiological detection capabilities and other countermeasures | |
| Assess and evaluate nuclear, biological, chemical, and radiological detection capabilities and other countermeasures | |
| **Overall assessment of progress** | **Limited** |

Source: GAO analysis.

- DHS's **acquisition management** efforts include managing the use of contracts to acquire goods and services needed to fulfill or support the agency's missions, such as information systems, new technologies, aircraft, ships, and professional services. As shown in table 10, we identified 3 performance expectations for DHS in the area of acquisition management and found that DHS has generally achieved 1 of them and has generally not achieved 2 others.

Table 10: Summary of Our Assessments for DHS's Acquisition Management Performance Expectations

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **1** |
| Assess and organize acquisition functions to meet agency needs | |
| **Generally not achieved** | **2** |
| Develop clear and transparent policies and processes for all acquisitions | |
| Develop an acquisition workforce to implement and monitor acquisitions | |
| **Overall assessment of progress** | **Modest** |

Source: GAO analysis.

- DHS's **financial management** efforts include consolidating or integrating component agencies' financial management systems. As shown in table 11, we identified 7 performance expectations for DHS in the area of financial management and found that DHS has generally achieved 2 of them and has generally not achieved 5 others.

**Table 11: Summary of Our Assessments for DHS's Financial Management Performance Expectations**

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **2** |
| Designate a department Chief Financial Officer who is appointed by the President and confirmed by the Senate | |
| Prepare corrective action plans for internal control weaknesses | |
| **Generally not achieved** | **5** |
| Subject all financial statements to an annual financial statement audit | |
| Obtain an unqualified financial statement audit opinion | |
| Substantially comply with federal financial management system requirements, applicable federal accounting standards, and the U.S. Standard General Ledger at the transaction level | |
| Obtain an unqualified opinion on internal control over financial reporting | |
| Correct internal control weaknesses | |
| **Overall assessment of progress** | **Modest** |

Source: GAO analysis.

- DHS's key **human capital management** areas include pay, performance management, classification, labor relations, adverse actions, employee appeals, and diversity management. As shown in table 12, we identified 8 performance expectations for DHS in the area of human capital management and found that DHS has generally achieved 2 of them and has generally not achieved 6 others.

Table 12: Summary of Our Assessments for DHS's Human Capital Management Performance Expectations

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **2** |
| Develop a results-oriented strategic human capital plan | |
| Create a comprehensive plan for training and professional development | |
| **Generally not achieved** | **6** |
| Implement a human capital system that links human capital planning to overall agency strategic planning | |
| Develop and implement processes to recruit and hire employees who possess needed skills | |
| Measure agency performance and make strategic human capital decisions | |
| Establish a market-based and more performance-oriented pay system. | |
| Seek feedback from employees to allow for their participation in the decision-making process | |
| Implement training and development programs in support of DHS's mission and goals | |
| **Overall assessment of progress** | **Limited** |

Source: GAO analysis.

- DHS's **information technology management** efforts include developing and using an enterprise architecture, or corporate blueprint, as an authoritative frame of reference to guide and constrain system investments; defining and following a corporate process for informed decision making by senior leadership about competing information technology investment options; applying system and software development and acquisition discipline and rigor when defining, designing, developing, testing, deploying, and maintaining systems; establishing a comprehensive, departmentwide information security program to protect information and systems; having sufficient people with the right knowledge, skills, and abilities to execute each of these areas now and in the future; and centralizing leadership for extending these disciplines throughout the organization with an empowered Chief Information Officer. As shown in table 13, we identified 13 performance expectations for DHS in the area of information technology management and found that DHS has generally achieved 2 of them and has generally not achieved 8 others. For 3 performance expectations, we could not make an assessment.

Table 13: Summary of Our Assessments for DHS's Information Technology Management Performance Expectations

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **2** |
| Organize roles and responsibilities for information technology under the Chief Information Officer | |
| Develop policies and procedures to ensure protection of sensitive information | |
| **Generally not achieved** | **8** |
| Develop a strategy and plan for information technology management | |
| Develop measures to assess performance in the management of information technology | |
| Implement a comprehensive enterprise architecture | |
| Develop a process to effectively manage information technology investments | |
| Implement a process to effectively manage information technology investments | |
| Develop policies and procedures for effective information systems development and acquisition | |
| Implement policies and procedures for effective information systems development and acquisition | |
| Implement policies and procedures to effectively safeguard sensitive information | |
| **No assessment made** | **3** |
| Strategically manage information technology human capital | |
| Develop a comprehensive enterprise architecture | |
| Provide operational capabilities for information technology infrastructure and applications | |
| **Overall assessment of progress** | **Limited** |

Source: GAO analysis.

- DHS's responsibilities for **real property management** are specified in Executive Order 13327, "Federal Real Property Asset Management," and include establishment of a senior real property officer, development of an asset inventory, and development and implementation of an asset management plan and performance measures. As shown in table 14, we identified 9 performance expectations for DHS in the area of real property management and found that DHS has generally achieved 6 of them and has generally not achieved 3 others.

Table 14: Summary of Our Assessments for DHS's Real Property Management Performance Expectations

| Performance expectation | Total |
|---|---|
| **Generally achieved** | **6** |
| Establish a Senior Real Property Officer who actively serves on the Federal Real Property Council | |
| Complete and maintain a comprehensive inventory and profile of agency real property | |
| Provide timely and accurate information for inclusion in the governmentwide real property inventory database | |
| Develop an Office of Management and Budget-approved asset management plan | |
| Establish an Office of Management and Budget-approved 3-year rolling timeline with certain deadlines by which the agency will address opportunities and determine its priorities as identified in the asset management plan | |
| Establish real property performance measures | |
| **Generally not achieved** | **3** |
| Demonstrate steps taken toward implementation of the asset management plan | |
| Use accurate and current asset inventory information and real property performance measures in management decision making | |
| Ensure the management of agency property assets is consistent with the agency's overall strategic plan, the agency asset management plan, and the performance measures | |
| **Overall assessment of progress** | **Moderate** |

Source: GAO analysis.

A variety of cross-cutting themes have affected DHS's efforts to implement its mission and management functions. These key themes include agency transformation, strategic planning and results management, risk management, information sharing, and partnerships and coordination.

- In past work, we reported on the importance of integration and transformation in helping DHS ensure that it can implement its mission and management functions. We designated the implementation and transformation of DHS as a high-risk area in 2003 and continued that designation in our 2005 and 2007 updates. As of May 2007, we reported that DHS had yet to submit a corrective action plan to the Office of Management and Budget. We reported that the creation of DHS is an enormous management challenge and that DHS faces a formidable task in its transformation efforts as it works to integrate over 170,000 federal employees from 22 component agencies. We noted that it can take a minimum of 5 to 7 years until organizations complete their transformations.

- We have identified strategic planning and the development and use of outcome-based performance measures as two of the key success factors for the management of any organization. DHS issued a departmentwide strategic plan that met most of the required elements for a strategic plan and is planning to issue an updated plan. However, we have reported that some component agencies have had difficulties in developing outcome-based goals and measures for assessing program performance. For example, in August 2005 we reported that U.S. Immigration and Customs Enforcement (ICE) had not yet developed outcome goals and measures for its worksite enforcement program, and in March 2006 we reported that U.S. Citizenship and Immigration Services (USCIS) had not yet established performance goals and measures to assess its benefit fraud activities. We have also noted that DHS faces inherent challenges in developing outcome-based goals and measures to assess the affect of its efforts on strengthening homeland security.

- We have also reported on the importance of using a risk management approach to set homeland security priorities and allocate resources accordingly. The *National Strategy for Homeland Security* and DHS's strategic plan have called for the use of risk-based decisions to prioritize DHS's resource investments, and risk management has been widely supported by the President, Congress, and the Secretary of Homeland Security as a management approach for homeland security. In past work we found that while some DHS component agencies, such as the Coast Guard and the Transportation Security Administration (TSA), have taken steps to apply risk-based decision making in implementing some of their mission functions, other components have not utilized such an approach. For example, we reported that DHS has not applied a risk management approach in deciding whether and how to invest in specific capabilities for preparing for and responding to catastrophic threats.

- In 2005 we designated information sharing for homeland security as high-risk. We recently reported that more than 5 years after September 11, 2001, the nation still lacked an implemented set of governmentwide policies and processes for sharing terrorism-related information and the area remained high-risk. However, we noted that the federal government has issued a strategy for how it will put in place the overall framework and policies for sharing information with critical partners and that DHS has taken actions to implement its information sharing responsibilities. For example, DHS has implemented an information system to share homeland security information and has supported the efforts of states and localities to create information “fusion” centers. We have reported that DHS faces challenges in continuing to develop productive information sharing relationships with federal agencies, state and local governments, and the private sector.

- We have also reported on the important role that DHS plays in partnering and coordinating its homeland security efforts with federal, state, local, private sector, and international stakeholders. The *National Strategy for Homeland Security* underscores the importance of DHS partnering with other stakeholders, as the majority of the strategy’s initiatives are intended to be implemented by three or more federal agencies. Our prior work has shown that, among other things, successful partnering and coordination involve collaborating and consulting with stakeholders to develop goals, strategies, and roles. DHS has taken steps to strengthen partnering frameworks and capabilities. For example, DHS has formed a working group to coordinate the federal response to cyber incidents of national significance. However, we have also reported on difficulties faced by DHS in its partnership efforts. For example, DHS faced challenges in coordinating with its emergency preparedness and response partners in the wake of Hurricanes Katrina and Rita due to, among other things, unclear designations of partners’ roles and responsibilities.

Given DHS’s dominant role in securing the homeland, it is critical that the department’s mission and management programs are operating as efficiently and effectively as possible. DHS has taken important actions to secure the border and transportation sectors and to prepare for and respond to disasters. DHS has had to undertake these missions while also working to transform itself into a fully functioning cabinet department—a difficult task for any organization. As DHS moves forward, it will be important for the department to continue to develop more measurable goals to guide implementation efforts and to enable better accountability of its progress toward achieving desired outcomes. It will also be important for DHS to continually reassess its mission and management goals, measures, and milestones to evaluate progress made, identify past and emerging obstacles, and examine alternatives to address those obstacles and effectively implement its missions.

In its comments on a draft of this report, DHS took issues with our methodology and disagreed with our assessments for 42 of 171 performance expectations. DHS’s five general issues were (1) perceptions that we altered our standards used to judge the department's progress; (2) concerns with the binary approach we used to assess the performance expectations; (3) concerns regarding perceived changes in criteria after DHS provided additional information; (4) concerns with consistency in our application of the methodology; and (5) concerns regarding our treatment of performance expectations as having equal weight. With regard to the first issue, as we communicated to DHS, we did not change our criteria; rather we made a change in language to better convey the intent behind the performance expectations that DHS achieve them instead of merely taken actions that apply or relate to them. Second, regarding our use of a binary standard to judge whether or not DHS generally met each of 171 performance expectations, we acknowledge the limitations of this standard, but believe it is appropriate for this review given the administration has generally not established quantitative goals and measures for the 171 expectations, which are necessary to systematically assess where along a spectrum of progress DHS stood in achieving each performance expectation. We applied a scale to assess different levels of progress made by DHS for its overall mission and management areas. With regard to the third issue, what DHS perceives as a change in criteria for certain performance expectations is not a change in criteria but simply the process by which we disclosed our preliminary assessment to DHS, analyzed additional documents and information from DHS, and updated and, in some cases revised, our assessments based on this additional input. Fourth, regarding concerns with consistency in our methodology application, our core team of GAO analysts and managers reviewed all inputs from GAO staff to ensure consistent application of our methodology, criteria, and analytical process. Finally, regarding concerns with our treatment of performance expectations as having equal weight, we acknowledge that differences exist between expectations, but we did not weight the performance expectations because congressional, departmental and others' views on the relative priority of each expectation may be different and we did not believe it was appropriate to substitute our judgment for theirs.

With regard to DHS's disagreement with our assessments for 42 of the performance expectations, DHS generally contends that (1) we expected DHS to have achieved an entire expectation in cases when that ultimate achievement will likely take several more years, and (2) we did not adequately use or appropriately interpret additional information DHS provided. In general, we believe that it is appropriate, after pointing out the expectation for a multiyear program and documenting the activities DHS has actually accomplished to date, to reach a conclusion that DHS has not yet fully implemented the program. We also believe we have appropriately used the documents DHS has provided us. In some cases, the information and documents DHS provided were not relevant to the specific performance expectation; in these situations we did not discuss them in our assessment. In other cases, the information did not convince us that DHS had achieved the performance expectation as stated or as we had interpreted it. In the assessment portion of each performance expectation, we have described how we applied the information DHS provided to the performance expectation and describe the level of progress DHS has made.

Overall, we appreciate DHS's concerns and recognize that in a broad-based endeavor such as this, some level of disagreement is inevitable, especially at any given point in time. However, we have been as transparent as possible regarding our purpose, methodology, and professional judgments.

## Background

In July 2002, President Bush issued the *National Strategy for Homeland Security*. The strategy set forth overall objectives to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and assist in the recovery from attacks that may occur. The strategy set out a plan to improve homeland security through the cooperation and partnering of federal, state, local, and private sector organizations on an array of functions. The *National Strategy for Homeland Security* specified a number of federal departments, as well as nonfederal organizations, that have important roles in securing the homeland. In terms of federal departments, DHS was assigned a prominent role in implementing established homeland security mission areas.

In November 2002, the Homeland Security Act of 2002 was enacted into law, creating DHS. This act defined the department's missions to include preventing terrorist attacks within the United States; reducing U.S. vulnerability to terrorism; and minimizing the damages, and assisting in the recovery from, attacks that occur within the United States. The act also specified major responsibilities for the department, including to analyze information and protect infrastructure; develop countermeasures against chemical, biological, radiological, and nuclear, and other emerging terrorist threats; secure U.S. borders and transportation systems; and organize emergency preparedness and response efforts.

DHS began operations in March 2003. Its establishment represented a fusion of 22 federal agencies to coordinate and centralize the leadership of many homeland security activities under a single department.[20] According to data provided to us by DHS, the department's total budget authority was about $39 billion in fiscal year 2004, about $108 billion in fiscal year 2005, about $49 billion in fiscal year 2006, and about $45 billion in fiscal year 2007.[21] The President's fiscal year 2008 budget submission requests approximately $46 billion for DHS. Table 15 provides information on DHS's budget authority, as reported by DHS, for each fiscal year from 2004 though 2007.

**Table 15: DHS Budget Authority for Fiscal Years 2004 through 2007 in Thousands of Dollars, as Reported by DHS**

| DHS component agency/program | Fiscal year 2004 budget authority | Fiscal year 2005 budget authority | Fiscal year 2006 budget authority | Fiscal year 2007 budget authority |
|---|---:|---:|---:|---:|
| Departmental Operations | $394,435 | $527,257 | $610,473 | $626,123 |
| Analysis and Operations | | | $252,940 | $299,663 |
| DHS IG | $80,318 | $97,317 | $84,187 | 98,685 |
| U.S. Secret Service | $1,334,128 | $1,375,758 | $1,423,489 | $1,479,158 |
| U.S. Customs and Border Protection (CBP) | $5,994,287 | $6,520,698 | $7,970,695 | $9,344,781 |
| U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT)[a] | $328,053 | $340,000 | $336,600 | $362,494 |
| U.S. Immigration and Customs Enforcement (ICE) | $3,669,615 | $4,244,228 | $4,206,443 | $4,726,641 |
| U.S. Citizenship and Immigration Services (USCIS) | $1,549,733 | $1,775,000 | $1,887,850 | $1,985,990 |
| Transportation Security Administration (TSA) | $4,578,043 | $5,405,375 | $6,167,014 | $6,329,291 |

[20] These 22 agencies, offices, and programs were U.S. Customs Service; U.S. Immigration and Naturalization Service; Federal Protective Service; Transportation Security Administration; Federal Law Enforcement Training Center; Animal and Plant Health Inspection Service; Office for Domestic Preparedness; Federal Emergency Management Agency; Strategic National Stockpile and the National Disaster Medical System; Nuclear Incident Response Team; Domestic Emergency Support Team; National Domestic Preparedness Office; Chemical, Biological, Radiological, and Nuclear Countermeasures Program; Environmental Measures Laboratory; National BW Defense Analysis Center; Plum Island Animal Disease Center; Federal Computer Incident Response Center; National Communication System; National Infrastructure Protection Center; Energy Security and Assurance Program; Secret Service; and U.S. Coast Guard.

[21] The amounts reflect total budget authority amounts as reported to us by DHS. The amounts include annual and supplemental appropriations, rescissions, amounts reprogrammed or transferred, fee estimates, and mandatory amounts. The amounts do not reflect carryover or rescissions of unobligated balances.

| DHS component agency/program | Fiscal year 2004 budget authority | Fiscal year 2005 budget authority | Fiscal year 2006 budget authority | Fiscal year 2007 budget authority |
|---|---:|---:|---:|---:|
| U.S. Coast Guard | $7,097,405 | $7,853,427 | $8,782,689 | $8,729,152 |
| National Protection and Programs Directorate/Preparedness Directorate[a] | | | $678,395 | $618,577 |
| Counter-Terrorism Fund | $9,941 | $8,000 | $1,980 | |
| Federal Emergency Management Agency (FEMA) | $8,378,109 | $74,031,032 | $11,175,544 | $5,223,503 |
| FEMA: Office of Grant Programs[b] | $4,013,182 | $3,984,846 | $3,377,737 | $3,393,000 |
| Science and Technology Directorate | $912,751 | $1,115,450 | $1,487,075 | $973,109 |
| Domestic Nuclear Detection Office | | | | $480,968 |
| Border and Transportation Security Directorate[a] | $8,058 | $9,617 | | |
| Federal Law Enforcement Training Center | $191,643 | $226,807 | $304,534 | $275,279 |
| Information Analysis and Infrastructure Protection Directorate[a] | $834,348 | $887,108 | | |
| **Total** | **$39,374,049** | **$108,401,920**[c] | **$48,747,645** | **$44,946,414** |

Source: DHS.

Note: Data are rounded to the nearest thousand. Fiscal year 2007 amounts are as of January 31, 2007. The data reflect total budget authority amounts as reported to us by DHS. The amounts include annual and supplemental appropriations, rescissions, amounts reprogrammed or transferred, fee estimates, and mandatory amounts. The amounts do not reflect carryover or rescissions of unobligated balances.

[a] The Border and Transportation Security Directorate, the Information Analysis and Infrastructure Protection Directorate, and the US-VISIT program are legacy organizations within DHS. The functions of these organizations have been realigned through DHS reorganizations. In particular, in March 2007 US-VISIT was reorganized under the National Protection and Programs Directorate. The Border and Transportation Security Directorate included U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, the Transportation Security Administration, and the Federal Law Enforcement Training Center.

[b] The Office of Grant Programs has undergone several realignments. It was previously known as the Office of Grants and Training in the Preparedness Directorate, the Office of State and Local Government Coordination and Preparedness, and the Office for Domestic Preparedness.

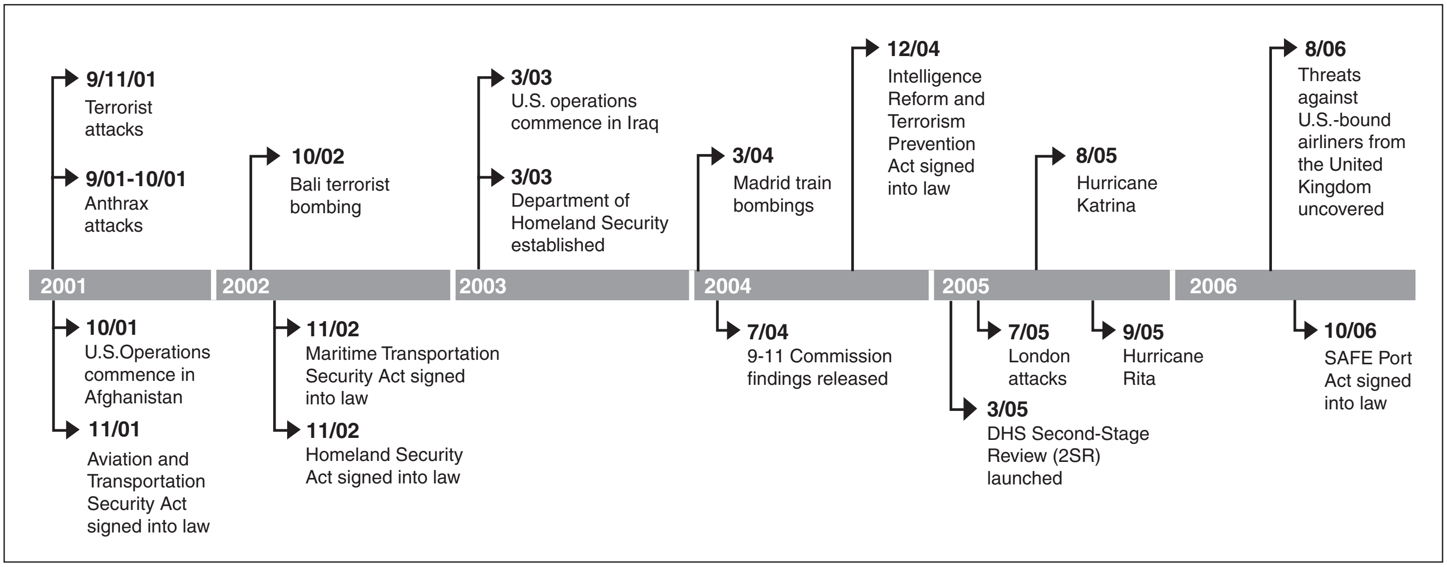
[c] The FEMA fiscal year 2005 amount includes about $45 billion in supplemental funding for Hurricane Katrina.

Since creating and issuing its first strategic plan, the department has undergone several reorganizations. Most notably, in July 2005, DHS announced the outcome of its Second-Stage Review, an internal study of the department's programs, policies, operations, and structures. As a result of this review, the department realigned several component agencies and functions. In particular, the Secretary of Homeland Security established a Directorate of Policy to coordinate departmentwide policies, regulations, and other initiatives and consolidated preparedness activities in one directorate, the Directorate for Preparedness. In addition, the Secretary established a new Office of Intelligence and Analysis and the Office of Infrastructure Protection composed of analysts from the former Information Analysis and Infrastructure Protection directorate. The Office of Infrastructure Protection was placed in the Directorate for Preparedness. The fiscal year 2007 DHS appropriations act provided for the further reorganization of functions within the department by, in particular, realigning DHS's emergency preparedness and response responsibilities.[22]

In addition to these reorganizations, a variety of factors have affected DHS's efforts to implement its mission and management functions. These factors include both domestic and international events, such as Hurricanes Katrina and Rita, and major homeland security-related legislation. Figure 2 provides a timeline of key events that have affected DHS's implementation.

[22] See Pub. L. No. 109-295, §§ 601-99, 120 Stat. 1355, 1394-1463 (2006).

**Figure 2: Selected Key Events That Have Affected Department of Homeland Security Implementation**


9/11/01
Terrorist attacks
9/01-10/01
Anthrax attacks
10/02
Bali terrorist bombing
3/03
U.S. operations commence in Iraq
3/03
Department of Homeland Security established
3/04
Madrid train bombings
12/04
Intelligence Reform and Terrorism Prevention Act signed into law
8/05
Hurricane Katrina
8/06
Threats against U.S.-bound airliners from the United Kingdom uncovered
2001
2002
2003
2004
2005
2006
10/01
U.S.Operations commence in Afghanistan
11/01
Aviation and Transportation Security Act signed into law
11/02
Maritime Transportation Security Act signed into law
11/02
Homeland Security Act signed into law
7/04
9-11 Commission findings released
7/05
London attacks
9/05
Hurricane Rita
3/05
DHS Second-Stage Review (2SR) launched
10/06
SAFE Port Act signed into law

Source: GAO analysis.

## DHS Has Made Varying Levels of Progress in Implementing its Core Mission and Management Functions, but Has Faced Difficulties in Its Implementation Efforts

Based on the performance expectations we identified, DHS has made progress in implementing its mission and management functions, but various challenges have affected its efforts. Specifically, DHS has made limited progress in the areas of emergency preparedness and response; science and technology; and human capital and information technology management. We found that DHS has made modest progress in the areas of border security; immigration services; and acquisition and financial management. We also found that DHS has made moderate progress in the areas of immigration enforcement, aviation security, surface transportation security; critical infrastructure and key resources protection, and real property management, and that DHS has made substantial progress in the area of maritime security.

### DHS Has Made Modest Progress in Border Security

The United States shares a 5,525 mile border with Canada and a 1,989 mile border with Mexico, and all goods and people traveling to the United States must be inspected at air, land, or sea ports of entry. In 2006, more than 400 million legal entries were made to the United States—a majority of all border crossings were at land border ports of entry. Within DHS, CBP is the lead agency responsible for implementing the department's border security mission. Specifically, CBP's two priority missions are (1) detecting and preventing terrorists and terrorist weapons from entering the United States, and (2) facilitating the orderly and efficient flow of legitimate trade and travel. CBP's supporting missions include interdicting illegal drugs and other contraband; apprehending individuals who are attempting to enter the United States illegally; inspecting inbound and outbound people, vehicles, and cargo; enforcing laws of the United States at the border; protecting U.S. agricultural and economic interests from harmful pests and diseases; regulating and facilitating international trade; collecting import duties; and enforcing U.S. trade laws. Within CBP, the United States Border Patrol is responsible for border security between designated official ports of entry, and CBP‘s Office of Field Operations enforces trade, immigration, and agricultural laws and regulations by securing the flow of people and goods into and out of the country, while facilitating legitimate travel and trade at U.S. ports of entry.

As shown in table 16, we identified 12 performance expectations for DHS in the area of border security and found that overall DHS has made modest progress in meeting those expectations. Specifically, we found that DHS has generally achieved 5 of its performance expectations and has generally not achieved 7 of its performance expectations.

Table 16: Performance Expectations and Progress Made in Border Security

| | Assessment | | |
|---|---|---|---|
| Performance expectation | Generally achieved | Generally not achieved | No assessment made |
| 1. Implement a biometric entry system to prevent unauthorized border crossers from entering the United States through ports of entry | ✓ | | |
| 2. Implement a biometric exit system to collect information on border crossers leaving the United States through ports of entry | | ✓ | |
| 3. Develop a program to detect and identify illegal border crossings between ports of entry | ✓ | | |
| 4. Implement a program to detect and identify illegal border crossings between ports of entry | | ✓ | |
| 5. Develop a strategy to detect and interdict illegal flows of cargo, drugs, and other items into the United States | ✓ | | |
| 6. Implement a strategy to detect and interdict illegal flows of cargo, drugs and other items into the United States | | ✓ | |
| 7. Implement effective security measures in the visa issuance process | | ✓ | |
| 8. Implement initiatives related to the security of certain documents used to enter the United States | | ✓ | |
| 9. Provide adequate training for all border related employees | ✓ | | |
| 10. Develop staffing plans for hiring and allocating human capital resources to fulfill the agency's border security mission | ✓ | | |
| 11. Ensure adequate infrastructure and facilities | | ✓ | |
| 12. Leverage technology, personnel, and information to secure the border | | ✓ | |
| **Total** | **5** | **7** | **0** |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

Table 17 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of border security and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation's key elements (generally not achieved).

Table 17: Performance Expectations and Assessment of DHS Progress in Border Security

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Implement a biometric entry system to prevent unauthorized border crossers from entering the United States through ports of entry | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. According to DHS, the entry portion of US-VISIT has been deployed at 154 of 170 land ports of entry, 115 airports, and 14 seaports, as of December 2006. With regard to 14 of the 16 land ports of entry where US-VISIT was not installed, CBP and US-VISIT program office officials told us there was no operational need for US-VISIT because visitors who are required to be processed into US-VISIT are, by regulation, not authorized to enter the United States at these locations. We reported that US-VISIT needs to be installed at the remaining 2 ports of entry in order to achieve full implementation as required by law, but both of these locations present significant challenges to installation of US-VISIT. These ports of entry do not currently have access to appropriate communication transmission lines to operate US-VISIT. CBP officials told us that, given this constraint, they determined that they could continue to operate as before. CBP officials told us that having US-VISIT biometric entry capability generally improved their ability to process visitors required to enroll in US-VISIT because it provided them additional assurance that visitors are who they say they are and automated the paperwork associated with processing the I-94 arrival/departure form. For more information, see *Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry,* GAO-07-248. | Generally achieved |
| 2. Implement a biometric exit system to collect information on border crossers leaving the United States through ports of entry | *GAO findings:* DHS has faced challenges in deploying a biometric exit system at ports of entry. Legislation required US-VISIT to collect biometric exit data from all individuals who are required to provide biometric entry data, but did not set a specific deadline for this requirement. Although US-VISIT had set a December 2007 deadline for implementing exit capability at the 50 busiest land ports of entry, US-VISIT has since determined that implementing an exit capability by this date is no longer feasible. A new date for exit implementation has not been set. In March 2007, we reported that DHS has devoted considerable time and resources toward establishing an operational exit capability. Over the last 4 years, it has committed over $160 million to pilot test and evaluate an exit solution at 12 air, 2 sea, and 5 land ports of entry. Despite this considerable investment of time and resources, the US-VISIT program still does not have either an operational exit capability or a viable exit solution to deploy to all air, sea, and land ports of entry. With regard to air and sea ports of entry, we reported that although US-VISIT has pilot tested a biometric exit capability for these ports of entry, it has not been available at all ports. A pilot test in 2004 through 2005 identified issues that limited the operational effectiveness of the solution, such as the lack of traveler compliance with the processes. According to program officials, US-VISIT is now developing a plan for deploying a comprehensive, affordable exit solution at all ports of entry. However, no time frame has been established for this plan being approved or implemented. There are interrelated logistical, technological, and infrastructure constraints that have precluded DHS from achieving this mandate, and there are cost factors related to the feasibility of implementation of such a solution. With regard to land ports of entry, for example, we reported that the major constraint to performing biometric verification upon exit at this time, in the US-VISIT Program Office's view, is that the only proven technology available would necessitate mirroring the processes currently in use for US-VISIT at entry. The US-VISIT Program Office concluded in January 2005 that the mirror-imaging solution was "an infeasible alternative for numerous reasons, including but not limited to, the additional staffing demands, new infrastructure requirements, and potential trade and commerce impacts." US-VISIT officials stated that they believe that technological advances over the next 5 to 10 years will make it possible to utilize alternative | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | technologies that provide biometric verification of persons exiting the country without major changes to facility infrastructure and without requiring those exiting to stop and/or exit their vehicles, thereby precluding traffic backup, congestion, and resulting delays. For more information, see GAO-07-248 and *Homeland Security: US-VISIT Program Faces Operational, Technological and Management Challenges,* GAO-07-632T.<br>*DHS updated information:* Between March and June 2007, DHS told us that, it expected that further land exit testing may be conducted in fiscal year 2008. DHS reported that it provided an exit strategy to Congress in the spring of 2007.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although DHS is continuing to explore various possibilities for implementing an exit capability, the department has not yet implemented a biometric exit system at land, air, and sea ports of entry. | |
| 3. Develop a program to detect and identify illegal border crossings between ports of entry | *GAO findings:* DHS has made progress toward developing a program to detect illegal border crossings between ports of entry. In February 2007, we reported that the Secure Border Initiative is a comprehensive, multiyear program established in November 2005 by the Secretary of Homeland Security to secure U.S. borders and reduce illegal immigration. The Secure Border Initiative's mission is to promote border security strategies that help protect against and prevent terrorist attacks and other transnational crimes. Elements of the Secure Border Initiative will be carried out by several organizations within DHS. One element of the Secure Border Initiative is SBI*net*, the program within CBP responsible for developing a comprehensive border protection system. SBI*net* is responsible for leading the effort to ensure that the proper mix of personnel, tactical infrastructure, rapid response capability, and technology is deployed along the border. According to DHS, the SBI*net* solution is to include a variety of sensors, communications systems, information technology, tactical infrastructure (roads, barriers, and fencing), and command and control capabilities to enhance situational awareness of the responding officers. The solution is also to include the development of a common operating picture that provides uniform data, through a command center environment, to all DHS agencies and is interoperable with stakeholders external to DHS. We have ongoing work to further assess the Secure Border Initiative. For more information, see GAO-07-248 and *Secure Border Initiative: SBI*net *Expenditure Plan Needs to Better Support Oversight and Accountability,* GAO-07-309.<br>*DHS updated information:* According to updated information provided by DHS between March and May 2007, the Secure Border Initiative program is in place, with a Program Management Office and governance structure, system integrator, and funding. In September 2006, the SBI*net* contract was awarded. CBP has been designated as the DHS executive agent for the SBI*net* program and has established a Program Management Office to oversee SBI*net*. With regard to other border security initiatives, DHS noted that Operation Streamline, launched in December 2005, is a coordinated effort among CBP, ICE, and the Department of Justice to create a zero-tolerance zone for illegal entries in the Del Rio Border Patrol sector.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has made progress in developing a strategy to detect and identify illegal border crossings between ports of entry—namely the Secure Border Initiative—and has developed other initiatives to detect and deter illegal border crossings. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 4. Implement a program to detect and identify illegal border crossings between ports of entry | *GAO and DHS IG findings:* DHS has not yet fully implemented a program to effectively detect and identify illegal border crossings between ports of entry. In past work, we and the DHS IG identified challenges in implementing earlier border security programs designed to detect and deter illegal border crossings. For example, in February 2006 the DHS IG reported that initiatives using technology, such as unmanned aerial vehicles and remote video surveillance, had failed to consistently demonstrate the predicted force multiplier effect for border security. More recently, we reported that although DHS has published some information on various aspects of the Secure Border Initiative and SBI*net*, it remains unclear how SBI*net* will be linked, if at all, to US-VISIT so that the two systems can share technology, infrastructure, and data across programs. In addition, we reported that according to DHS, work on the northern border for the Secure Border Initiative is not projected to begin before fiscal year 2009. We have ongoing work to further assess the Secure Border Initiative. For more information, see GAO-07-309; GAO-07-248; *Border Security: Key Unresolved Issues Justify Reevaluation of Border Surveillance Technology Program,* GAO-06-295; and *Border Security: Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands,* GAO-04-590. Also, see Department of Homeland Security Office of the Inspector General, *A Review of Remote Surveillance Technology Along U.S. Land Borders,* OIG-06-15 (Washington, D.C.: December 2005).<br>*DHS updated information:* DHS provided evidence of SBI*net* progress, including the award of four task orders as of May 2007. At the end of fiscal year 2006, DHS reported that 75 miles of fence were constructed and a total of 370 miles are planned to be constructed by the end of calendar year 2008. CBP also plans to establish 200 miles of vehicle barriers by the end of calendar year 2008, with 67 miles completed. Further, DHS has established a Miles of Effective Control goal. The goal is to gain effective control of the entire southwest border by 2013. According to DHS, effective control indicates that defense-in-depth capabilities in the area are robust enough to (1) detect illegal entries; (2) identify and classify the entries; (3) efficiently and effectively respond; and (4) bring events to a satisfactory law enforcement resolution. As of March 2007, DHS reported that it had 392 miles under effective control, and the goal for the end of calendar year 2008 is 642 miles. DHS stated that SBI*net* Technology Coverage goal is to cover 387 miles of the border completed by the end of calendar year 2008 in the Tucson and Yuma sectors. With regard to Operation Streamline, CBP reported that beginning with a 5-mile stretch of the border, the initiative now spans the entire 210 mile Del Rio Sector Border. DHS also noted that National Guard resources have been deployed to the border to enhance capabilities under Operation Jumpstart. As of February 28, 2007, DHS reported that nearly 46,000 aliens were apprehended and more than 520 vehicles were seized through Operation Jumpstart. Additionally, CBP plans to add 6,000 Border Patrol agents by the end of calendar year 2008. In fiscal year 2007, DHS plans to increase its Border Patrol presence between ports of entry by hiring, training, and deploying 1,500 additional agents.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. The Secure Border Initiative and SBI*net* are in the early phases of implementation, and DHS has taken actions to implement the initiative, particularly in awarding four task orders under SBI*net*. However, these contracts have only recently been awarded, and it is unclear what progress contractors have made in implementing the activities specified in the task orders. Moreover, DHS reported that it has effective control of 380 miles of the border as of March 2007, but the U.S. land border encompasses more than 6,000 miles, and DHS does not expect to begin work on the northern border until fiscal year 2009. Although DHS has only recently begun to implement SBI*net*, which is a multi-year program, DHS and its legacy components implemented programs to secure the border between ports of entry prior to the Secure Border Initiative and SBI*net*. We and the DHS IG reported on challenges faced by DHS in implementing programs that pre-dated the Secure Border Initiative and SBI*net*. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 5. Develop a strategy to detect and interdict illegal flows of cargo, drugs, and other items into the United States | *GAO findings:* DHS has taken steps to develop a strategic approach for interdicting illegal flows of cargo, drugs, and other items into the United States.[a] For example, according to DHS, in August 2006 DHS and the Department of Justice submitted a National Southwest Border Counternarcotics Strategy and Implementation Plan to the International Drug Control Policy Coordinating Committee. This document identified the major goals, objectives, and resource requirements for closing gaps in U.S. and Mexico counternarcotics capabilities along the southwest border. DHS has also taken steps to plan for the deployment of radiation portal monitors at ports of entry. For more information, see *Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports-of-Entry, but Concerns Remain,* GAO-06-389; *Prescription Drugs: Strategic Framework Would Promote Accountability and Enhance Efforts to Enforce the Prohibitions on Personal Importation,* GAO-05-372; and *Cigarette Smuggling: Federal Law Enforcement Efforts and Seizures Increasing,* GAO-04-641.<br>*DHS updated information:* According to updated information provided by DHS, the CBP Office of Field Operations developed a comprehensive strategic plan entitled Securing America's Borders at the Ports of Entry that defines CBP's national strategy specifically at all air, land, and sea ports of entry. This plan was finalized and published in September 2006 concurrent with the development of the Secure Border Initiative. According to DHS, it complements the national strategy for gaining operational control of the borders between ports of entry and addresses the specific security concerns and required actions that are the direct responsibility of the Office of Field Operations. Programs under the auspices of the Office of Field Operations that support enhanced detection and interdiction of illegal flows of contraband and harmful substances into the United States include the National Targeting Center for Cargo; the Automated Targeting System; the Customs Trade Partnership Against Terrorism; the Container Security Initiative; the Secure Freight Initiative; and deployment of radiation portal monitors, large-scale, non-intrusive inspection technology, and canine enforcement teams. Additionally, according to the Office of Counternarcotics, in March 2006, the National Southwest Border Counternarcotics Strategy was approved by the International Drug Control Policy Coordinating Committee. This document identified the major goals, objectives, and recommendations for closing gaps in U.S. and Mexico counternarcotics capabilities along the southwest border.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has made progress in developing a strategy to implement its various programs for detecting and interdicting illegal flows of cargo, drugs, and other items into the United States. With regard to flows of illegal drugs in particular, the National Southwest Border Counternarcotics Strategy has been approved by the International Drug Control Policy Coordinating Committee. | Generally achieved |
| 6. Implement a strategy to detect and interdict illegal flows of cargo, drugs, and other items into the United States | *GAO findings:* We have identified challenges in DHS's efforts to interdict flows of illegal goods into the United States.[b] DHS has implemented the Container Security Initiative to allow CBP officials to target containers at foreign seaports so that any high-risk containers maybe inspected prior to their departure for the United States. We have identified challenges in implementation of the program, including staffing imbalances that, in the past, impeded CBP's targeting of containers. DHS has also implemented the Customs-Trade Partnership Against Terrorism, a voluntary program design to improve the security of international supply chain through which CBP officials work in partnership with private companies to review supply chain security plans. Our work has identified a number of challenges in implementation of the Customs-Trade Partnership Against Terrorism, including that CBP's standard for validation is hard to achieve and, given that the program is voluntary, there are limits on how intrusive CBP can be in its validations. With regard to radiation portal monitors, we reported as of December 2005, DHS had completed deployment of portal monitors at two categories of entry—a total of 61 ports of entry—and had begun work on two other categories; overall, however, progress had been slower than planned. According to DHS officials, the slow progress resulted from a late disbursal of funds and delays in negotiating deployment agreements with seaport | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | operators. Further, we noted the expected cost of the program was uncertain because DHS's plans to purchase newer, more advanced equipment were not yet finalized, and we projected that the program's final cost would be much higher than CBP anticipated at the time of our review. In 2006, we reported on the results of our investigation of potential security weaknesses associated with the installation of radiation detection equipment at ports of entry. As part of this investigation, we deployed two teams of investigators to the field to make simultaneous border crossings at the northern and southern borders in an attempt to transport radioactive sources into the United States. The radiation portal monitors properly signaled the presence of radioactive material when our two teams of investigators conducted simultaneous border crossings. Our investigators' vehicles were inspected in accordance with most of the CBP policy at both the northern and southern borders. However, our investigators, using counterfeit documents, were able to enter the United States with the radioactive sources in the trunks of their vehicles. In 2005 we also reported that inspection and interdiction efforts at international mail branches and express carrier facilities had not prevented a reported substantial volume of prescription drugs from being illegally imported from foreign Internet pharmacies into the United States. We acknowledged that CBP and other agencies, including ICE, the Food and Drug Administration, and the Drug Enforcement Administration, had taken a step in the right direction by collaborating to establish a task force designed to address challenges that we identified, but nonetheless, an unknown number of illegal drugs entered the country each day. In addition, in 2004 we noted that CBP reported that the number of cigarette seizures by CBP and ICE increased dramatically, from 12 total seizures in 1998 to 191 seizures in 2003. CBP attributed this increase to better intelligence and better inspections—based on electronic methods such as its Automated Targeting System. For more information, see GAO-06-389; GAO-05-372; GAO-04-641; *Border Security: Investigators Transported Radioactive Sources Across Our Nation's Borders at Two Locations*, GAO-06-940T; and *Maritime Security: Observations on Selected Aspects of the SAFE Port Act*, GAO-07-754T.<br>*DHS updated information:* DHS provided updated information related to its implementation of a strategy to detect and interdict illegal flows of cargo, drugs, and other items into the United States. In general, the Strategic Plan on *Securing America's Borders at the Ports of Entry,* which defines CBP's national strategy at all air, land, and sea ports of entry, outlines programs designed to achieve border security objectives. CBP's Office of Field Operations has developed a formal implementation process to execute the Securing America's Borders at the Ports of Entry strategic plan that includes regular senior executive participations, steering committee oversight, and the creation of *Securing America's Borders at the Ports of Entry* Implementation Division to provide ongoing oversight and coordination of a comprehensive development schedule for the Office of Field Operations' high priority programs. More specifically, DHS has several programs in place to help detect and interdict illegal flows of cargo, drugs, and other items into the United States. These programs include the National Targeting Center for Cargo, the Automated Targeting System, the Customs-Trade Partnership Against Terrorism, the Container Security Initiative, deployment of radiation portal monitors, large-scale non-intrusive inspection technology, canine enforcement programs, and the Secure Freight Initiative.[c] With regard to the National Targeting Center for Cargo, CBP reported that this center expands CBP's capability to do cargo shipment targeting to provide ports of entry with immediate analysis capabilities. With regard to radiation portal monitors, as of March 9, 2007, CBP has deployed 966 radiation portal monitors to ports of entry. According to CBP, these radiation portal monitor deployments provide CBP with the capability to screen approximately 91 percent of containerized cargo and 88 percent of personally owned vehicles entering the United States. With regard to non-intrusive technology, CBP reported deploying about 189 systems and is scheduled to have 224 large-scale systems deployed by the end of fiscal year 2009. CBP's canine enforcement teams are assigned to 73 ports of entry and more than 300 detector dog teams were trained in fiscal year 2006. DHS provided us with other sensitive data on the outputs of its efforts, which we considered in making our assessment. Furthermore, according to the Office of Counternarcotics, the Implementation Plan for the | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | National Southwest Border Counternarcotics Strategy includes recommendations on funding and resource requirements and estimated timelines for implementing the National Southwest Border Counternarcotics Strategy in fiscal years 2008 through 2011. In addition, in fiscal year 2007, DHS plans to increase its Border Patrol presence between ports of entry by hiring, training, and deploying 1,500 additional agents.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has taken actions to implement various programs to detect and interdict illegal flows of goods into the United States. For example, DHS has deployed radiation portal monitors and large scale non-intrusive detection systems at ports of entry and has developed the Container Security Initiative and Customs-Trade Partnership Against Terrorism Program. However, we have reported on challenges in implementation efforts associated with these programs. Moreover, CBP's *Securing America's Borders at the Ports of Entry* plan is still in the early stages of implementation, but once implemented, will help CBP detect and interdict illegal flows of goods into the United States. Further, the Implementation Plan for the National Southwest Border Counternarcotics Strategy has only recently been developed. In addition, we considered the sensitive data provided by DHS on the outputs of its efforts as well as our prior work in making our assessment. | |
| 7. Implement effective security measures in the visa issuance process | *GAO findings:* DHS has made progress but still faces challenges in its efforts to implement effective security measures as part of the visa issuance process.[d] In 2005 we reported that DHS had not yet expanded the Visa Security Program as it planned. The Visa Security Program is DHS's program to oversee the assigning of visa security officers to locations overseas to review visa applications. In prior work we reported that DHS had begun supplying Visa Security Officers to the U.S. embassy and consulate in Saudi Arabia. According to DHS, the Department of State's consular officials, and the deputy chief of mission in Saudi Arabia, the Visa Security Officers strengthened visa security at these posts. Visa Security Officers offer law enforcement and immigration experience and have access to and experience using information from law enforcement databases, which are not readily available to consular officers. DHS planned to expand the Visa Security Program to additional posts throughout fiscal years 2005 and 2006, but faced various difficulties in its efforts to expand. For example, chiefs of mission at the posts chosen for expansion in fiscal year 2005 delayed approval of DHS's requests. Embassy and Department of State officials attributed the delays to questions about the program's goals, objectives, and staffing requirements, as well as DHS's plans to coordinate with existing law enforcement and border security staff and programs at post at that time. For more information, see *Border Security: Actions Needed to Strengthen Management of Department of Homeland Security's Visa Security Program,* GAO-05-801.<br>*DHS updated information:* Since the time of our review, DHS has made progress in expanding the Visa Security Program to additional posts.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although the department has made some progress in expanding the Visa Security Program, the department has reported facing similar challenges to those that we previously identified in its expansion and implementation efforts and did not provide us with evidence that it has fully addressed those challenges. | Generally not achieved |
| 8. Implement initiatives related to the security of certain documents used to enter the United States | *GAO findings:* DHS has various initiatives related to the security of documents used to enter the United States but has faced difficulties in implementing these initiatives.[e] With regard to the Western Hemisphere Travel Initiative, we reported in May 2006 on challenges faced by DHS in implementation. This initiative is DHS's program to implement requirements for U.S. citizens and citizens of Bermuda, Canada, and Mexico to show a passport or other documents that the Secretary of Homeland Security deems sufficient to show identity and citizenship to CBP officers when those individuals enter the United States from certain countries in North, Central, or South America. We reported that alternative programs or documents, such as frequent traveler programs and driver's licenses with enhanced security features, had various | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | challenges and using them in lieu of a passport would not easily resolve the management issues faced by DHS. We reported that once decisions are made on what documents will be needed, DHS and the Department of State will face challenges in program implementation and management. Major challenges would remain in developing (1) an implementation plan, (2) budget estimates, (3) awareness programs for the public, (4) training programs for DHS staff, (5) bilateral coordination with Canada, and (6) a common understanding of how the Travel Initiative links to the overall strategy for securing the nation's borders. Falling short in any of these areas may hinder the ability of the agencies to achieve their goal of improving security while facilitating commerce and tourism. According to DHS officials, they have formed working groups to take action in each of these areas, but much more work remains in developing plans and approaches that improve the likelihood of program success.<br>With regard to the Visa Waiver Program, the 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. In July 2004, we reported that DHS established a Visa Waiver Program Oversight Unit, which completed security assessments of the 27 countries that participate in the Visa Waiver Program. DHS also submitted a report to Congress summarizing the assessment findings. However, we identified several problems with the 2004 review process, as key stakeholders were not consulted during portions of the process, the review process lacked clear criteria and guidance to make key judgments, and the final reports were untimely. Furthermore, the monitoring unit could not effectively achieve its mission to monitor and report on ongoing law enforcement and security concerns in visa waiver countries due to insufficient resources. In September 2006 we testified that while DHS had taken some actions to mitigate the program's risks, the department faced difficulties in further mitigating these risks. In particular, the department had not established time frames and operating procedures regarding timely stolen passport reporting—a program requirement since 2002. Furthermore, DHS sought to require the reporting of lost and stolen passport data to the United States and the International Criminal Police Organization, but it had not issued clear reporting guidelines to participating countries.<br>With regard to the Immigration Advisory Program, this pilot program is designed to increase the level of scrutiny given to the travel documents of certain high-risk passengers before they board international flights traveling to the United States. Under this program, CBP assigns officers to selected foreign airports where they utilize an automated risk-targeting system that identifies passengers as potentially high-risk—including passengers who do not need a visa to travel to the United States. CBP officers then personally interview some of these passengers and evaluate the authenticity and completeness of these passengers' travel documents. CBP has reported several successes through the Immigration Advisory Program pilot. According to CBP documents, from the start of the program in June 2004 through February 2006, Immigration Advisory Program teams made more than 700 no-board recommendations for inadmissible passengers and intercepted approximately 70 fraudulent travel documents. However, in May 2007 we reported that CBP had not taken all of the steps necessary to fully learn from its pilot sites in order to determine whether the program should be made permanent and the number of sites that should exist. These steps are part of a risk management approach to developing and evaluating homeland security programs.<br>In addition, in prior work our agents have attempted to enter the United States using fictitious documents. Our periodic tests since 2002 clearly showed that CBP officers were unable to effectively identify counterfeit driver's licenses, birth certificates, and other documents. Specifically, in 2003 our agents were able to easily enter the United States from Canada and Mexico using fictitious names and counterfeit driver's licenses and birth certificates. Later in 2003 and 2004, we continued to be able to successfully enter the United States using counterfeit identification at land border crossings, but were denied entry on one occasion. In 2006, the results of our work indicated that CBP officers at the nine land border crossings we tested at that time did not detect the counterfeit identification we used. At the time of our | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | review, CBP agreed that its officers were not able to identify all forms of counterfeit identification presented at land border crossings and fully supported the Western Hemisphere Travel Initiative that will require all travelers to present a passport before entering the United States. We did not assess whether this initiative would be effective in preventing terrorists from entering the United States or whether it would fully address the vulnerabilities shown by our work. We have ongoing work assessing the Western Hemisphere Travel Initiative and the use of fraudulent travel documents. For more information, see GAO-07-248; *Border Security: Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program*, GAO-06-854; *Observations on Efforts to Implement the Western Hemisphere Travel Initiative on the U.S. Border with Canada*, GAO-06-741R; *Border Security: Consular Identification Cards Accepted within United States, but Consistent Federal Guidance Needed*, GAO-04-881; *Aviation Security: Efforts to Strengthen International Passenger Prescreening Are Under Way, but Planning and Implementation Issues Remain*, GAO-07-346; and *Border Security: Continued Weaknesses in Screening Entrants into the United States*, GAO-06-976T.<br>*DHS updated information:* According to updated information provided by DHS, CBP has undertaken a variety of efforts associated with the security of documents used to enter the United States. These efforts include implementation of the Western Hemisphere Travel Initiative in the air environment; enhancements to the Visa Waiver Program; increased access to lost and stolen passport information from multiple sources; introduction of the Fraudulent Documents Analysis Unit, which issues notices to the field regarding detection of fraudulent documents; and training of carrier agents overseas in documentary requirements and fraudulent document detection. With regard to the Western Hemisphere Travel Initiative, since January 23, 2007, all U.S. citizens and nonimmigrant aliens from Canada, Bermuda and Mexico entering the United States from within the Western Hemisphere at air ports of entry are required to present a valid passport. CBP has reported more than 99 percent compliance with these requirements at air ports of entry. DHS stated that the department is working toward implementation of the Western Hemisphere Travel Initiative for travelers entering the United States through land and sea ports of entry, and in June 2007 announced the Notice of Proposed Rulemaking for the land and sea portions. U.S. and Canadian citizens entering the United States from within the Western Hemisphere at land and sea ports currently may make a verbal declaration of citizenship or present a myriad of forms and documents to enter the country such as birth certificates and drivers' licenses. On June 8, 2007, because of delays in processing applications for U.S. passports, U.S. citizens traveling to Canada, Mexico, the Caribbean, and Bermuda who have applied for but not yet received passports can temporarily enter and depart from the United States by air with a government issued photo identification and Department of State official proof of application for a passport through September 30, 2007. With regard to fraudulent documents, CBP reported that it has electronic copies of all U.S.-issued travel and citizenship documents, with the exception of U.S.-issued passports, which CBP is working to gain access to with the Department of State. When travelers apply for admission at a port of entry, CBP officers are to scan the document presented by the travelers to help minimize the risk of photograph substitution on the documents and the use of canceled travel documents. Over 4,400 CBP officers have access to the Department of State Consolidated Consular Database, which allows officers to view unique visa information. During 2006, CBP stated that it provided ports of entry with the highest rate of fraudulent document interceptions with comprehensive document examination workstations to better equip them with the ability to examine questioned documents presented for entry to the United States. According to CBP, workstations have been deployed at 11 ports of entry, where the equipment improves the ability of officers to thoroughly inspect documents to detect forgeries. CBP reported that its Fraudulent Document Analysis Unit received 40,362 fraudulent documents from the ports of entry during fiscal year 2006. Of this number, there were 7,252 passports from 84 countries, the majority of which were issued by Mexico and the United States. CBP also reported that it has deployed ePassport readers to 200 primary inspection lanes at the 33 largest airports to enhance document verification. With regard to lost and stolen passports, | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | DHS reported that it has a real-time interface with the State Department that provides data on all lost or stolen passports reported to the State Department, both United States and foreign. CBP noted that the programs mentioned above are used in conjunction with US-VISIT fingerprinting of non-U.S. citizens and resident aliens to provide a biometric authentication of the document-bearers' identity and verification of documents' validity. With regard to the Immigration Advisory Program, DHS has issued a strategic plan for fiscal years 2007 through 2012.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has taken actions related to the security of certain documents used to enter the country by, for example, implementing the Western Hemisphere Travel Initiative at air ports of entry. However, we have reported on management challenges faced by DHS with regard to the Western Hemisphere Travel Initiative and, although the requirement for implementing the initiative is not until 2009, we reported that the Departments of Homeland Security and State have a long way to go to implement their proposed plans, and the time to get the job done has been slipping by. We have also reported on risks and challenges faced by DHS with regard to the Visa Waiver Program, such as the timely reporting of stolen passports, and DHS did not provide us with evidence that it has taken actions to fully address these risks and challenges. Furthermore, while DHS has made progress in deploying document examination workstations and ePassport readers to lanes at ports of entry, DHS did not provide us with evidence that it has yet determined proposed locations for deploying additional workstations. In addition, DHS has not yet fully used a risk management approach in implementing its Immigration Advisory Program. | |
| 9. Provide adequate training for all border related employees | *GAO findings:* DHS has taken steps to provide training to border security personnel. In September 2005, we reported that the creation of CBP within DHS merged border inspection functions at U.S. ports of entry, which had previously been performed by three separate agencies. We reported that the "One Face at the Border," initiative created the positions of CBP officer and CBP agriculture specialist and combined aspects of three former inspector functions. CBP created a series of training courses to provide former U.S. Customs and former Immigration and Naturalization Service officers with the knowledge and skills necessary to carry out the responsibilities of this new position. In addition, CBP officers received training to meet CBP's new mission priority of terrorism prevention. Because agricultural inspections were more specialized, CBP officers received training sufficient to enable them to identify potential agricultural threats, make initial regulatory decisions, and determine when to make referrals to CBP agriculture specialists. We reported that CBP emphasized on-the-job training in an effort not to place officers on the job without direct supervisory and tutorial backup. CBP's main strategy to prepare for field delivery of training was to provide extensive train-the-trainer courses so that trainers could return to their field sites and instruct officers there. We reported that change had not come about without challenges, as many officers were reported to have resisted changes to their responsibilities, mainly related to the difficulties in learning a new set of procedures and laws. Officials noted that there has been an enormous amount of required training for CBP officers, and it could sometimes be overwhelming. For former officers, in addition to completing an extensive cross-training schedule and new training related to terrorism prevention, there were many other required courses related to their mission. We reported that although staffing challenges may ultimately have been relieved with trained officers able to perform dual inspections, officials noted that it had been extremely difficult to take staff off-line to complete the "One Face at the Border" training. In March 2007, we reported that Border Patrol's basic training program exhibited attributes of an effective training program. However, we also reported while Border Patrol officials were confident that the academy could accommodate the large influx of new trainees anticipated over the next 2 years, they have expressed concerns over the sectors' ability to provide sufficient field training. For example, officials were concerned with having a sufficient number of experienced agents available in the sectors to serve as field training officers and first-line supervisors. We | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | reported that the Border Patrol is considering several alternatives to improve the efficiency of basic training delivery and to return agents to the sectors more quickly. For example, the Border Patrol is pilot-testing a proficiency test for Spanish that will allow those who pass the test to shorten their time at the academy by about 30 days. However, we concluded that the Border Patrol's plan to hire an unprecedented number of new agents over the next 2 years could strain the sectors' ability to provide adequate supervision and training. Moreover, the field training new agents receive has not been consistent from sector to sector, a fact that has implications for how well agents perform their duties. To ensure that these new agents become proficient in the safe, effective, and ethical performance of their duties, it will be extremely important that new agents have the appropriate level of supervision and that the Border Patrol has a standardized field training program. For more information, see *Department of Homeland Security: Strategic Management of Training Important for Successful Transformation*, GAO-05-888 and *Homeland Security: Information on Training New Border Patrol Agents*, GAO-07-540R.<br>*DHS updated information:* In May 2007, DHS provided us with updated information on its efforts to provide training for border security personnel. Specifically, CBP reported that it has implemented a plan to hire and train 3,900 Border Patrol agents in fiscal year 2007; 4,800 agents in fiscal year 2008; and 850 agents in the first quarter of fiscal year 2009. CBP, working with the Federal Law Enforcement Training Center, reported making various modifications to the Border Patrol basic training program to accommodate the volume of new trainees. CBP also reported that it is designing its post-Academy training to align with the new Academy program and to use the 2-year Federal Career Intern Program. In addition, CBP has an annual call for training and uses a National Training Plan and a Training Advisory Board to determine ongoing basic and advanced training requirements. Post-Academy training for Border Patrol Agents includes a structured academic program with two pass or fail probationary exams, and Border Patrol local offices provide agents with area-specific training through the Border Patrol Field Training Program. Post-Academy training for CBP officers working at ports of entry feature classroom, online, and on-the-job experiences linked to the job that the individual CBP officer will perform in his or her home duty post. According to CBP, CBP provides in-depth, task-based training to CBP officers that address tasks that the CBP officer will be called on to perform. In addition, CBP provides "cross-training" to officers from the former U.S. Immigration and Naturalization Service or Customs Services based on operational requirements.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. CBP has established and implemented programs for training its border security personnel. With regard to basic training, we previously reported that Border Patrol's basic training program exhibited attributes of an effective training program. CBP also uses a National Training Plan and a Training Advisory Board to determine training requirements. However, in prior work we reported on various challenges in CBP's provision and adequacy of field-based training. For example, with regard to Border Patrol agents, we reported that the field training new agents receive has not been consistent from sector to sector, which has implications for how well agents perform their duties. In addition, we identified concerns regarding CBP's capacity to provide training to the projected large influx of new Border Patrol agents over the next 2 years. | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 10. Develop staffing plans for hiring and allocating human capital resources to fulfill the agency's border security mission | *GAO findings:* CBP has taken actions to develop staffing plans for hiring and allocating human capital resources to fulfill the agency's border security mission. In July 2005 we reported that CBP had taken steps to increase management flexibility in assigning staff to inspection functions and improve staff allocation in an effort to minimize passenger wait times and ensure the most efficient use of existing staff at airports. We reported that CBP had introduced its "One Face at the Border" program to increase staffing flexibility so that staff could conduct different types of inspections within airports. We also reported that CBP was developing a national staffing model to more systematically allocate existing staff levels at airports nationwide, however, the model did not address weaknesses identified in Customs' and U.S. Immigration and Naturalization Service's staffing models in our and the Department of Justice Inspector General's previous audit work. In February 2006, we reported that for program acquisitions like the America's Shield Initiative to be successful, DHS needed to, among other things, have adequate staff to fill positions that have clearly defined roles and responsibilities and that it had not fully staffed the America's Shield Initiative program office. One criticism we had of the former U.S. Immigration and Naturalization Service was that because of staffing shortages, mission staff often had to assume administrative or other functions as a collateral duty. One effect of assigning mission staff to administrative work was that they were not spending all of their time on duties needed to accomplish the program's mission and thus were not reaching the full potential of the program position. In 2005 we found that this was a problem in some offices. Some officials we contacted in CBP said they had to use mission staff in this way because they did not have enough administrative support to compensate for the realignment of administrative staff to shared services, the addition of mission personnel that came as a result of mergers of some programs in the transition, and hiring freezes. As a result, officers, adjudicators, and investigators in some field offices were taking on administrative work full-time or as a collateral duty. For more information, see GAO-06-295 and *Homeland Security: Management Challenges Remain in Transforming Immigration Programs,* GAO-05-81.<br>*DHS updated information:* In May 2007, DHS provided us with data on CBP's fiscal year 2007 hiring projections and documentation of its staffing models for various positions within CBP, such as CBP officers and Border Patrol agents. Information on these staffing models is sensitive.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed staffing models and plans for border security personnel. | Generally achieved |
| 11. Ensure adequate infrastructure and facilities | *GAO findings:* DHS has not yet satisfactorily ensured that CBP inspectors and Border Patrol have adequate infrastructure and facilities to support their activities. CBP Field Operations maintains programs at 20 field operations offices and 327 ports of entry, of which 15 are pre-clearance stations in Canada and the Caribbean. Border Patrol agents are assigned to patrol more than 6,000 miles of the nation's land borders and are coordinated through 20 sectors. CBP's facilities and tactical infrastructure portfolio consisted of CBP-owned and leased facilities and real estate; temporary structures, such as modular buildings for rapid deployment and temporary base camps; and other tactical infrastructure, such as fences, lights, and barriers. Additionally, CBP owned and maintained a motor vehicle fleet; a variety of aircraft including fixed wing aircraft, helicopters, and unmanned aerial vehicles; and different types of marine vessels such as hovercrafts, airboats, and high-speed interceptors. Further, the agency acquired different types of scanning and detection equipment, such as large-scale x-ray and gamma-imaging systems, nuclear and radiological detection equipment, as well as a variety of portable and hand-held devices. In February 2007, we reported that CBP's capital planning process was evolving and not yet mature. Although the agency has established a review and approval framework that required documentation to (1) describe how a proposed capital project supports the agency's strategic goals and (2) identify the mission need and gap between current and required capabilities, we were unable to verify implementation of these practices due to a lack of non-information technology examples. Additionally, we reported that CBP has | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | not developed a comprehensive, agencywide, long-term capital plan, although it produced several documents that included some elements of such a plan. For land ports of entry, CBP implemented a capital investment planning process to ensure that facility and real property funding is allocated in a manner that supports critical facility projects. CBP piloted the capital investment planning process and the strategic resource assessments on the land port of entry. In December 2006, we reported that with regard to US-VISIT going forward, DHS plans to introduce changes and enhancements to US-VISIT at land ports of entry, including a transition from digitally scanning 2 fingerprints to 10. While such changes are intended to further enhance border security, deploying them may have an impact on aging and space-constrained land ports of entry facilities because they could increase inspection times and adversely affect port of entry operations. Moreover, our previous work showed that the US-VISIT program office had not taken necessary steps to help ensure that US-VISIT entry capability operates as intended. For example, in February 2006 we reported that the approach taken by the US-VISIT program office to evaluate the impact of US-VISIT on land port of entry facilities focused on changes in I-94 processing time at 5 ports of entry and did not examine other operational factors, such as US-VISIT's impact on physical facilities or work force requirements. As a result, program officials did not always have the information they needed to anticipate problems that occurred, such as problems processing high volumes of visitors in space constrained facilities. For more information please see GAO-07-248 and *Federal Capital: Three Entities' Implementation of Capital Planning Principles is Mixed.* GAO-07-274.<br>*DHS updated information:* In May 2007, DHS provided updated information outlining steps it has and is taking to improve land ports of entry inspection and Border Patrol facilities so they effectively meet mission requirements. CBP plans to extend the methodology piloted on land ports of entry to air and sea ports of entry by the end of 2007. According to DHS, its fiscal year 2007 to 2011 Construction Spending Plan includes a rapid response component to address urgent facility requirements for the 6,000 new Border Patrol agents who will be deployed between fiscal year 2007 and December 2008 as well as the existing facility gap for 3,400 currently deployed agents. According to DHS, the focus of the rapid response effort is the Border Patrol Stations, which will accommodate the vast majority of new agents. Border Patrol sector headquarters, checkpoints, horse stables, and remote processing facilities are included in CBP's investment strategy, but not in the rapid response solutions since they are minimally affected by the increase in deployment.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. According to DHS, there is an existing facility gap for 3,400 currently deployed Border Patrol agents, and although DHS is planning a rapid response to a legislative mandate requiring a large staffing increase by the end of 2008, DHS has not yet sufficiently increased infrastructure and facilities. Furthermore, as we previously reported, DHS's capital investment planning process is not yet mature and has only been piloted at the land ports of entry. In addition, with regard to US-VISIT, we reported on various infrastructure-related difficulties which could affect effective implementation of the program. | |
| 12. Leverage technology, personnel, and information to secure the border | *GAO and DHS IG findings:* DHS has worked to leverage its resources to secure the border, but has faced challenges in doing so. For example, CBP's Interagency Border Inspection System has sought to improve screening of travelers entering the United States at ports of entry by utilizing terrorist information that the National Terrorist Screening Center gathers and consolidates. The DHS IG reported, though, that the name-based watch lists that this system utilizes had been prone to repeated false hits for the same individual on different trips, a situation that results in CBP officers conducting secondary inspections of the travelers every time they enter the United States, an inefficient use of the officers' time. In addition, in December 2006 we reported that DHS has not yet articulated how US-VISIT is to strategically fit with other land-border security initiatives and mandates, and thus cannot ensure that these programs work in harmony to meet mission goals and operate cost effectively. We noted that agency programs need to properly fit within a common strategic context governing key aspects | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | of program operations, such as what functions are to be performed, what facility or infrastructure changes will be needed to ensure that they operate in harmony and as intended, and what standards govern the use of technology. We reported that until decisions on DHS's border security initiatives are made, it remains unclear how programs will be integrated with US-VISIT, if at all—raising the possibility that CBP would be faced with managing differing technology platforms and border inspection processes at each land port of entry. We reported that knowing how US-VISIT is to work in concert with other border security and homeland security initiatives and what facility or facility modifications might be needed could help Congress, DHS, and others better understand what resources and tools are needed to ensure success. For more information, see GAO-07-248 and *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public,* GAO-06-1031. Also, see Department of Homeland Security Office of Inspector General, *Review of CBP Actions Taken to Intercept Suspected Terrorists at U.S. Ports of Entry,* OIG-06-43 (Washington, D.C.: June 2006).<br>*DHS updated information:* In April 2007, DHS reported that its Interagency Border Inspection System and US-VISIT are well integrated at air, sea and land border ports. According to CBP, CBP officers at these ports of entry are able to screen travelers against both biographic and biometric watch lists in addition to verifying identities and travel documents. CBP reported that false hits on watch lists have been addressed with an enhancement that allows port personnel to identify the subjects if false hits in the system to prevent hits on subsequent trips. US-VISIT and other border and port systems utilize the same architecture and infrastructure to minimize costs and promote information sharing. Additionally, DHS stated that the Secure Border Initiative Strategic Plan is bringing clarity of mission, effective coordination of DHS assets, and greater accountability to the work of DHS in securing the nation's borders. Moreover, according to DHS, Operation Streamline, launched in December 2005, is a coordinated effort among CBP, ICE, and the Department of Justice to create a zero tolerance zone for illegal entries in the Del Rio Office of Border Patrol sector. Beginning with a 5 mile stretch of the border, Operation Streamline now spans the entire 210 mile Del Rio Sector Border.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although DHS has taken some actions to leverage technology, personnel, and information to secure the border, such as using watch lists, more work remains. For example, it is still unclear how US-VISIT will work with other border security initiatives, including the Secure Border Initiative. While the Secure Border Strategic Plan provides some information on how the various border security initiatives relate, the plan does not fully describe how these initiatives will interact once implemented. In addition, the further development and implementation of SBI*net* will be key to DHS efforts in achieving this performance expectation, but SBI*net* is still in the early phases of implementation. | |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

[a] In addition to DHS, other agencies, such as the Department of Justice, have a role to play in developing a strategy to detect and interdict illegal flows of goods in the country. This performance expectation is focused on DHS's roles and responsibilities in developing a strategy for detecting and interdicting illegal flows of goods into the United States.

[b] In addition to DHS, other agencies, such as the Department of Justice, have a role to play in detecting and interdicting illegal flows of goods in the country. This performance expectation is focused on DHS's roles and responsibilities in implementing a strategy for detecting and interdicting illegal flows of goods into the United States. We address cargo security in the context of maritime security in a later section of this report.

[c] We address those programs related to maritime cargo security, for example the Customs-Trade Partnership Against Terrorism and the Container Security Initiative, in a later section of this report.

[d] In addition to DHS, other agencies, such as the Department of State, have a role to play in implementing effective security measures in the visa issuance process. This performance expectation is focused on DHS's roles and responsibilities in implementing effective security measures in the visa issuance process—namely the Visa Security Program.

[e] Other agencies, such as the Department of State, have responsibilities for enhancing the security of documents used to enter the United States.

## DHS Has Made Moderate Progress in Immigration Enforcement

DHS is responsible for enforcing U.S. immigration laws. Immigration enforcement includes apprehending, detaining, and removing criminal and illegal aliens; disrupting and dismantling organized smuggling of humans and contraband as well as human trafficking; investigating and prosecuting those who engage in benefit and document fraud; blocking and removing employers' access to undocumented workers; and enforcing compliance with programs to monitor visitors. Within DHS, ICE is primarily responsible for immigration enforcement efforts. In particular, ICE's Office of Investigations is responsible for enforcing immigration and customs laws and its Office of Detention and Removal Operations is responsible for processing, detaining, and removing aliens subject to removal from the United States.

As shown in table 18, we identified 16 performance expectations for DHS in the area of immigration enforcement, and we found that overall DHS has made moderate progress in meeting those expectations.[23] Specifically, we found that DHS has generally achieved 8 of the performance expectations and has generally not achieved 4 other performance expectations.[24] For 4 performance expectations, we could not make an assessment. In meeting its performance expectations, ICE faced budget constraints that significantly affected its overall operations during fiscal year 2004. For example, ICE was faced with a hiring freeze in fiscal year 2004 that affected its ability to recruit, hire, and train personnel. Over the

[23] We did not include DHS's trade enforcement functions, such as export enforcement, in our review because we have completed limited work in this area.

[24] DHS undertakes these efforts in accordance with the Immigration and Nationality Act of 1952, as amended. See generally 8 U.S.C. § 1101 et seq.

past 2 years, ICE has reported taking actions to strengthen its immigration enforcement functions and has, for example, hired and trained additional personnel to help fulfill the agency's mission.

Table 18: Performance Expectations and Progress Made in Immigration Enforcement

| Performance expectation | Assessment | | |
|---|---|---|---|
| | Generally achieved | Generally not achieved | No assessment made |
| 1. Develop a program to ensure the timely identification and removal of noncriminal aliens subject to removal from the United States | ✓ | | |
| 2. Implement a program to ensure the timely identification and removal of noncriminal aliens subject to removal from the United States | | ✓ | |
| 3. Ensure the removal of criminal aliens | | ✓ | |
| 4. Assess and prioritize the use of alien detention resources to prevent the release of aliens subject to removal | ✓ | | |
| 5. Develop a program to allow for the secure alternative detention of noncriminal aliens | ✓ | | |
| 6. Implement a program to allow for the secure alternative detention of noncriminal aliens | | | ✓ |
| 7. Develop a prioritized worksite enforcement strategy to ensure that only authorized workers are employed | ✓ | | |
| 8. Implement a prioritized worksite enforcement strategy to ensure that only authorized workers are employed | | ✓ | |
| 9. Develop a comprehensive strategy to interdict and prevent trafficking and smuggling of aliens into the United States | ✓ | | |
| 10. Implement a comprehensive strategy to interdict and prevent trafficking and smuggling of aliens into the United States | | ✓ | |
| 11. Develop a law enforcement strategy to combat criminal alien gangs in the United States and cross-border criminal activity | ✓ | | |
| 12. Implement a law enforcement strategy to combat criminal alien gangs in the United States and cross-border criminal activity | | | ✓ |
| 13. Disrupt and dismantle mechanisms for money laundering and financial crimes | | | ✓ |
| 14. Develop a program to screen and respond to local law enforcement and community complaints about aliens who many be subject to removal | ✓ | | |
| 15. Develop staffing plans for hiring and allocating human capital resources to fulfill the agency's immigration enforcement mission | ✓ | | |
| 16. Provide training, including foreign language training, and equipment for all immigration enforcement personnel to fulfill the agency's mission | | | ✓ |
| **Total** | **8** | **4** | **4** |

Source: GAO analysis.

Note: An assessment of “generally achieved” indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of “generally achieved” does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, “generally not achieved” indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of “generally not achieved” may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated “no assessment made.”

Table 19 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of immigration enforcement and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation’s key elements (generally not achieved).

**Table 19: Performance Expectations and Assessment of DHS Progress in Immigration Enforcement**

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Develop a program to ensure the timely identification and removal of noncriminal aliens subject to removal from the United States | *GAO and DHS IG findings:* DHS has taken actions to develop programs to help ensure the timely identification and removal of noncriminal aliens subject to removal from the United States. In June 2003, ICE established the Compliance Enforcement Unit to reduce the number of aliens who had violated the terms of certain types of visas and were residing in the United States. According to the DHS IG, the National Security Entry-Exit Registration System, the Student and Exchange Visitor System, and the United States Visitor and Immigrant Status Indicator Technology identify visa violators. These three systems are designed to track a specific segment of the nonimmigrant population and provide ICE with information concerning visa overstays. The DHS IG reported that when compliance violations were identified, enforcement actions must identify, locate, and apprehend violators. Once apprehended, violators must be detained, adjudicated, and removed. We have ongoing work assessing DHS guidelines for removing aliens from the United States who are subject to removal. For more information, see Department of Homeland Security Office of Inspector General, *Review of the Immigration and Customs Enforcement’s Compliance Enforcement Unit,* OIG-05-50 (Washington, D.C: September 2005); *Detention and Removal of Illegal Aliens,* OIG-06-33 (Washington, D.C.: April 2006); *An Assessment of United States Immigration and Customs Enforcement’s Fugitive Operations Teams,* OIG-07-34 (Washington, D.C.: March 2007); and *Review of U.S. ICE’s Detainee Tracking Process,* OIG-07-08 (Washington, D.C.: November 2006).<br>*DHS updated information:* In March, April, and May 2007, ICE provided updated information on its efforts to ensure the timely identification and removal of aliens subject to removal from the United States. ICE established the National Fugitive Operations Program in fiscal year 2003 to reduce the number of fugitive aliens in the United States and established the Fugitive Operations Support Center in June 2006 to aid in accounting for and reporting on the U.S. fugitive alien population, reviewing cases in ICE’s Deportable Alien Control System, developing targeted field operational initiatives, assessing national absconder data, and providing comprehensive leads and other support to field offices. ICE reported establishing fiscal year goals for the Fugitive Operations Teams located throughout its field offices. Each field office, | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | based on the number of teams located within its area of operational responsibility, is expected to arrest 1,000 fugitive targets and targets' associates. Furthermore, the Fugitive Operations Support Center has a goal of eliminating another 26,000 fugitive cases annually as a result of data integrity updates to ICE's Deportable Alien Control System.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation as DHS has taken actions to develop a program to ensure the timely identification and removal of aliens subject to removal from the United States. | |
| 2. Implement a program to ensure the timely identification and removal of noncriminal aliens subject to removal from the United States | *GAO and DHS IG findings:* Various factors have affected DHS's efforts to identify and remove noncriminal aliens subject to removal from the United States in a timely manner. According to the DHS IG, in recent years the number of "other than Mexican" aliens that DHS has apprehended has been rising, and such aliens have consumed more ICE resources because they cannot simply be returned over the border. In April 2006, the DHS IG found that Detention and Removal Operations was unable to ensure the departure from the United States of all removable aliens. In April 2006, the DHS IG reported that of the 774,112 illegal aliens apprehended during the prior 3 years, 280,987 (36 percent) were released largely due to a lack of personnel, bed space, and funding needed to detain illegal aliens while their immigration status was being adjudicated. The DHS IG noted that their release presented a significant risk due to the inability of CBP and ICE to verify the identity, country of origin, and terrorist or criminal affiliation of many of the aliens being released. Further, the DHS IG reported that the declining personnel and bed space level was occurring when the number of illegal aliens apprehended was increasing. The DHS IG stated that even though the Detention and Removal Operations had received additional funding and enhanced its Fugitive Operations Program, it was unlikely that many of the released aliens would ever be removed. ICE has encountered trouble deporting other than Mexican aliens because it has to first obtain travel documents from the aliens' countries of origin in order to repatriate them, and some countries have been unwilling to issue these documents. The DHS IG found that this unwillingness on the part of the countries of origin to issue travel documents created a "mini-amnesty" program for some aliens and also encouraged aliens to enter the United States illegally if they knew that their countries did not cooperate. DHS reported that it was working with the Department of State to address travel documents and related issues preventing or impeding the repatriation of aliens, particularly to Central and South American countries. However, the DHS IG reported that these efforts had yet to fully address the potential national security and public safety risks associated with DHS's inability to remove tens of thousands of illegal aliens. In addition, in March 2007, the DHS IG reported on DHS's National Fugitive Operations Program. The purpose of the program is to identify, locate, apprehend, and remove aliens—both criminal and noncriminal—who have unexecuted final orders of removal. This program analyzes data contained in various systems, such as the Student and Exchange Visitor Information System that contains information on international students and exchange visitors, to identify those who may have violated their terms of entry or who might otherwise pose a threat to national security. The DHS IG found that the backlog of fugitive aliens increased despite Fugitive Operation Teams' efforts and that the teams' efforts were hampered by insufficient detention capacity; database limitations; and inadequate working space. Additionally, the DHS IG reported that the removal rate of fugitive aliens apprehended by the teams could not be determined. The DHS IG noted that progress had been made in staffing the teams and that the teams had effective partnerships with federal, state, and local agencies. We have ongoing work assessing DHS guidelines for removing aliens from the United States who are subject to removal. For more information, see Department of Homeland Security Office of | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | Inspector General, *Detention and Removal of Illegal Aliens,* OIG-06-33 (Washington, D.C.: April 2006); *An Assessment of United States Immigration and Customs Enforcement's Fugitive Operations Teams,* OIG-07-34 (Washington, D.C.: March 2007); and *Review of U.S. ICE's Detainee Tracking Process,* OIG-07-08 (Washington, D.C.: November 2006).<br>*DHS updated information:* In March, April, and May 2007, ICE provided data on the results of its efforts to implement a program to ensure the timely identification and removal of aliens subject to removal from the United States. According to DHS, under the Secure Border Initiative, DHS has ended "catch and release" of non-Mexican nationals apprehended at or near U.S. borders. DHS stated that it remains committed to a "catch and return" regime, ensuring that no alien is released due to lack of detention capacity in fiscal years 2006 and 2007. DHS also reported that the average length of time spent in detention by an alien during removal proceedings has generally decreased from about 41.5 days in fiscal year 2002 to about 33.7 days as of August 31, 2006. However, ICE reported that during the first 5 months of fiscal year 2007, the average length of stay increased to 38.5 days. ICE officials noted that various factors can affect the average length of stay, such as the unwillingness of foreign countries to issue travel documents and the type pf proceeding in which an alien is placed (e.g., expedited removal or a full hearing).[a] ICE also stated that increased use of electronic travel documents and video teleconferencing have helped reduce delays that have contributed to longer periods of detention. ICE officials noted that decisions by foreign countries to refuse or delay issuance of travel documents are outside the control of DHS, and ICE has stationed a full-time liaison officer at the Department of State to help improve relations with the Department of State and foreign countries. ICE reported that it has improved relations with Central American countries in particular regarding the issuance of travel documents and noted, for example, that El Salvador, Guatemala, and Honduras—which are among the countries with the highest number of removals from the United States—have agreed to use ICE's Electronic Travel Document System. With regard to its National Fugitive Operations Program, ICE reported that at the end of fiscal year 2006, it had deployed 50 Fugitive Operations Teams nationwide and noted that 75 such teams have been fully funded for fiscal year 2007. Additional information reported by ICE on its effort to identify and remove criminal aliens from the United States is provided under the next performance expectation.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has undertaken efforts to ensure the timely identification of aliens subject to removal from the United States and provided us with data on its efforts, including data on the number of removable aliens arrested. DHS also provided us with data on the average length of time spent in detention by aliens during removal proceedings. While the average length of stay has generally decreased over time, DHS still faces difficulties in ensuring the removal of all aliens subject to removal from the United States in a timely manner. First, the average length of stay for an alien in detention between October 2006 and the end of February 2007 has increased from the fiscal year 2006 level; it remains to be seen whether the average of length of stay in fiscal year 2007 will increase, decrease, or stay the same as the fiscal year 2006 level. Second, the DHS IG reported that DHS has faced difficulties in removing aliens from the United States because of the unwillingness of some countries to provide the necessary travel documents, a circumstance that may be outside of DHS's control but that DHS has implemented efforts to help address, such as negotiating memoranda of understanding with foreign countries. DHS has finalized memorandum of understanding with three countries, and is working with other countries to expand use of the Electronic Travel Document System. Nevertheless, as previously suggested by | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | the DHS IG, these efforts may not yet fully address the potential national security and public safety risks associated with DHS's inability to remove tens of thousands of illegal aliens. Third, DHS has faced challenges in identifying aliens for removal from the United States and, according to the DHS IG, the fugitive alien population appears to be growing at a rate that exceeds Fugitive Operations Teams' ability to apprehend. | |
| 3. Ensure the removal of criminal aliens | *GAO and DHS IG findings:* Our work and the DHS IG's work have shown that DHS has faced difficulties in its efforts to ensure the removal of criminal aliens from the United States. In October 2004 we reported that although the legacy U.S. Immigration and Naturalization Service was to identify and remove criminal aliens as they came out of federal and state prison systems, it had failed to identify all removable imprisoned criminal aliens. Some who were released from prison committed and were convicted of new felonies. At that time, ICE Detention and Removal Operations officials, who took over the program from the Immigration and Naturalization Service, stated that they were taking steps to ensure the departure of all removable aliens. For example, they established fugitive operations teams. In April 2006, the DHS IG also reported that the expansion of the Criminal Alien Program, which identifies and processes criminal aliens incarcerated in federal, state, and local correctional institutions and jails who have no legal right to remain in the United States after serving out their sentence, would create more demands for the Detention and Removal Operations to detain, process, and remove illegal aliens. The DHS IG concluded that DHS and ICE needed to ensure that any planned increase in the Detention and Removal Operations' ability to identify and remove criminal aliens be accompanied by a comparable increase in support personnel, detention bed space, equipment, infrastructure, and funding to ensure the timely removal of criminal aliens from the United States. Besides the lack of bed space, the DHS IG reported that the Detention and Removal Operations' ability to detain and remove illegal aliens with final orders of removal was affected by (1) the propensity of illegal aliens to disobey orders to appear in immigration court; (2) the penchant of released illegal aliens with final orders to abscond; (3) the practice of some countries to block or inhibit the repatriation of its citizens; and (4) two U.S. Supreme Court decisions that mandate the release of criminal and other high-risk aliens 180 days after the issuance of the final removal order except in "Special Circumstances." The DHS IG reported that, collectively, the bed space, personnel, and funding shortages, coupled with the other factors, had created an unofficial "mini-amnesty" program for criminal and other high-risk aliens. For more information, see *Immigration Enforcement: DHS Has Incorporated Immigration Enforcement Objectives and Is Addressing Future Planning Requirements,* GAO-05-66. Also, see Department of Homeland Security Office of Inspector General, *Detention and Removal of Illegal Aliens,* OIG-06-33 (Washington, D.C.: April 2006); *An Assessment of United States Immigration and Customs Enforcement's Fugitive Operations Teams,* OIG-07-34 (Washington, D.C.: March 2007); and *Review of U.S. ICE's Detainee Tracking Process,* OIG-07-08 (Washington, D.C.: November 2006).<br>*DHS updated information:* During March, April, and May 2007, ICE provided updated information on its efforts to ensure the removal of criminal aliens from the United States. According to ICE, there are no data on the universe of aliens incarcerated in state and local jails who are amenable to removal proceedings. This is because prisons and jails utilize independent booking software that tracks place of birth in different ways. Additionally, information on place of birth is not sufficient to determine whether an individual is an alien subject to removal from the United States. According to ICE, while it does not know the exact number of incarcerated criminal aliens subject to removal at this time, there are approximately 158,000 incarcerated criminal aliens with immigration detainers within the Enforcement Operational Immigration | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | Records system, ICE's administrative case management system. In June 2006 and in support of its Criminal Alien Program, ICE established the National Detection Enforcement and Processing Offenders by Remote Technology Center in Chicago, Illinois to help in the screening, interviewing, and removal processing of criminal aliens in federal detention facilities throughout the United States to help ensure that these criminal aliens are deported rather than released into the community upon completion of their federal sentences. ICE reported that this center has screened more than 9,200 incarcerated criminal aliens, issued nearly 7,000 charging documents, and located nearly 1,000 alien absconders. Moreover, ICE reported that it has finalized agreements with nine local law enforcement agencies to work with these agencies to take into custody and remove aliens convicted of crimes at the state and local level. Using these partnerships and other measures, ICE reported that as of March 2007, its Criminal Alien Program has provided coverage for 1,674 of the 4,828 federal, state, and local jails and prisons nationwide, including for all 114 Bureau of Prisons federal detention facilities. ICE reported that for fiscal year 2007 it has set a target of removing 90,000 aliens from U.S. prisons and jails and, for fiscal year 2007, is on pace to double the approximately 60,000 charging documents it issued through the Criminal Alien Program in fiscal year 2006. ICE plans to expand coverage of the Criminal Alien Program to 3,400 covered facilities by fiscal year 2009. According to ICE, each Criminal Alien Program team is expected to process 1,800 new administrative cases per year. ICE also reported that from October 1, 2006, through March 31, 2007, it has removed more than 17,000 Bureau of Prison non-U.S. citizen inmates. If the bureau releases a similar number in fiscal year 2007 as it released in fiscal year 2006 (about 26,600, according to ICE), ICE reported that it is on track to remove all removable aliens released from the Bureau of Prisons in fiscal year 2007. Overall, ICE projects that in fiscal year 2007, it will process for removal more than 120,000 removable aliens located in prisons and jails nationwide.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although DHS has made progress in removing criminal aliens from the United States, much more work remains. For example, DHS has taken actions to expand its Criminal Alien Program to remove criminal aliens subject to removal from the United States after they complete their sentences in federal, state, and local correctional institutions and jails. However, ICE has not yet expanded the Criminal Alien Program or taken actions to ensure coverage of all federal, state, and local correctional institutions and jails. ICE has reached agreements with only nine local law enforcement agencies to remove aliens convicted of crimes at the state or local level. As a result, ICE may not be able to fully ensure the removal of criminal aliens from facilities that are not covered through the Criminal Alien Program or agreements with local law enforcement agencies. Moreover, the DHS IG reported that ICE faces a variety of challenges in its efforts to expand the Criminal Alien Program, and DHS did not provide us with evidence that it has yet addressed these challenges. | |
| 4. Assess and prioritize the use of alien detention resources to prevent the release of aliens subject to removal | *GAO and DHS IG findings:* DHS has taken actions to assess and prioritize use of alien detention and removal resources. In November 2005, the DHS IG reported that the separation of CBP's apprehension components from Detention and Removal Operations created challenges in national coordination because the two are part of different agencies that pursued different sets of priorities and each has its own planning process. The DHS IG noted that Detention and Removal Operations prepared detention bed space and staff needs projections without the benefit of CBP apprehension and arrest projections, while CBP developed its future apprehension initiatives without the benefit of insight into Detention and Removal Operations' future processing capability. In an effort to achieve better efficiency and effectiveness, ICE and CBP negotiated a memorandum of understanding between Border Patrol agents | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | and ICE investigators, although employees of both agencies noted persisting coordination problems in the apprehension and detention process. Other factors that increased the number of aliens that the Detention and Removal Operations have detained include the rising number of aliens that require mandatory detention and Detention and Removal Operations' improved ability to identify criminal aliens who are incarcerated in correctional institutions and jails and who will be subject to removal upon release from jail. The DHS IG also found that ICE has worked to improve strategic planning for detention resources, and the ICE Detention and Removal Operations issued a strategic plan in 2003 called "Endgame." This plan includes specific objectives for optimizing the means for detaining illegal aliens, including (1) ensuring sufficient and appropriate bed space is available based on detention category, characteristic, and condition of release; (2) enhancing partnerships with other federal detention agencies for better use of their resources, to include facilities and training; and (3) developing a National Custody Management Plan promoting the effective utilization of available bed space and alternative detention settings. The plan identified several significant challenges, many beyond DHS's control, including the number of aliens to remove, limited resources, political will, foreign governments, and nonremovable aliens. The DHS IG reported that, for these reasons, DHS needed to intensify its efforts to provide ICE with the resources and interagency support needed to overcome these challenges. For more information, see Department of Homeland Security Office of Inspector General, *An Assessment of the Proposal to Merge Customs and Border Protection with Immigration and Customs Enforcement,* OIG-06-04 (Washington, D.C.: November 2005); *ICE's Compliance with Detention Limits for Aliens with a Final Order of Removal from the United States*, OIG-07-28 (Washington, D.C.: February 2007); *Treatment of Immigration Detainees Housed at Immigration and Customs Enforcement Facilities,* OIG-07-01 (Washington, D.C.: December 2006); *Review of U.S. ICE's Detainee Tracking Process*, OIG-07-08 (Washington, D.C.: November 2006); and *Detention and Removal of Illegal Aliens,* OIG-06-33 (Washington, D.C.: April 2006).<br>*DHS updated information:* In March 2007, ICE provided updated information on efforts to assess and prioritize use of alien detention and removal resources. According to ICE, successful enforcement strategies and the requirement to manage within ICE's operational budget have resulted in a situation where Detention and Removal Operations has exceeded its funded bed space level and therefore must apply rigorous criteria to determine which apprehended aliens are detained. According to DHS, ICE detains all aliens who pose a threat to community safety or national security, and those required to be detained under the nation's immigration laws. In fiscal year 2006, ICE added 7,000 beds in facilities along the southern border, and in the first quarter of fiscal year 2007 added 2,000 beds. In order to ensure the availability of bed space in the future, ICE introduced a formal capacity planning program designed to provide advance notice of future bed space requirements and collaborated with apprehending entities to obtain apprehension forecasts to project short and long term needs. The Detention Operations Coordination Center, established in July 2006, coordinates the transfer of detainees from field offices with a shortage of detention space to those with available beds. ICE also reported that the detainee transportation system has been restructured to increase in-flight service routes for longer, more cost effective flights. ICE reported that as it creates models to determine detention capacity needs, Detention and Removal Operations is taking account of the capacity needs of CBP and ICE and is working with the U.S. Bureau of Prisons, U.S. Citizenship and Immigration Services, and the Departments of Justice and State to develop a more efficient detention and | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | removal system.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. While the availability of detention space depends on resources, DHS has taken actions to assess and prioritize the use of alien detention resources to prevent the release of aliens subject to removal by increasing bed space, relocating detainees, and better coordinating with relevant agencies. DHS has also taken actions to develop and implement a capacity planning program to identify future bed space requirements and has established priorities for bed space needs. | |
| 5. Develop a program to allow for the secure alternative detention of noncriminal aliens | *GAO findings:* DHS has made progress in developing programs to allow secure alternatives to detention. In October 2004, we reported that Detention and Removal Operations planned to use the results of its pilot programs (e.g., electronic monitoring and home visits of nondetained aliens) to determine which efforts intended to prevent nondetained aliens from fleeing while in immigration proceedings would merit additional funding.<br>*DHS updated information:* In March 2007, ICE provided updated information on its Intensive Supervision Appearance Program and its Electronic Monitoring Program. According to ICE, under the Intensive Supervision Appearance Program, established in June 2004 and only available to aliens not subject to mandatory detention, all participants must agree to comply with the conditions of their release. Case specialists are then assigned a limited caseload of participants and are responsible for monitoring those participants in the community by using tools such as electronic monitoring (bracelets), home visits, work visits, and reporting by telephone. The Electronic Monitoring Program is a reporting and case management tool for aliens released from custody that utilizes telephone reporting and electronic devices, such as radio frequency and Global Positioning System technology, to identify a nondetained alien's location and help ensure the alien's appearance at scheduled hearings and, as appropriate, the alien's scheduled removal. Last, DHS is conducting research on piloting a program that would utilize a kiosk-type hardware like the US-VISIT program to which an alien could report monthly. Instead of reporting to a deportation officer, the alien would scan his fingerprint and have his photo taken at the kiosk, which would be linked to appropriate databases.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed two programs that allow for the secure alternative detention of noncriminal aliens—the Intensive Supervision Appearance program and the Electronic Monitoring Program—and is exploring other alternatives to detention for noncriminal aliens. | Generally achieved |
| 6. Implement a program to allow for the secure alternative detention of noncriminal aliens | *GAO findings:* We have not conducted work on DHS's efforts to provide for the secure alternative detention of noncriminal aliens.<br>*DHS updated information:* In March 2007, ICE provided updated information on its efforts to provide alternatives to detention. ICE reported that under its Intensive Supervision Appearance Program there has been an 82 percent court appearance rate, as compared to 61 percent for the general nondetained population and that 47 percent of program-enrolled aliens who received final removal orders were confirmed to have left the United States compared to 13 percent of aliens in the nondetained general population believed to have compiled with removal orders. According to ICE, since the inception of the Electronic Monitoring Program in 2003, the program has been used by almost 9,100 aliens and is currently used by 6,500 aliens. ICE noted that the number of aliens who have participated in these programs has been relatively small and that only certain aliens are eligible to be detained through these programs. ICE noted that no limit exists on the total number of aliens who can be monitored under the program. Furthermore, ICE noted that it is | No assessment made |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | working to improve its alternative to detention programs by, for example, exploring additional supervision technologies and developing a memorandum of understanding with the Executive Office for Immigration Review to fast-track alternative-to-detention participants through the immigration hearing process. In addition, ICE reported that it is planning to expand its programs for secure alternative detention to increase programs' capacity to allow for a total detained population of 10,500 aliens.<br>*Our assessment:* We cannot assess of the extent to which DHS has generally achieved this performance expectation. We have not completed work related to DHS's effort to implement a program for secure alternatives to detention, and while DHS provided us with some information on its implementation efforts, we are unable to assess DHS's progress in achieving this performance expectation based on this information. | |
| 7. Develop a prioritized worksite enforcement strategy to ensure that only authorized workers are employed | *GAO findings:* Our work has shown that DHS has taken actions to develop a prioritized worksite enforcement program. As part of the Secure Border Initiative, in April 2006 ICE announced a new interior enforcement strategy to target employers of unauthorized aliens, immigration violators, and criminal networks. As we testified in June 2006, under this strategy, ICE has planned to target employers who knowingly employ unauthorized workers by bringing criminal charges against them. For more information, see *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts,* GAO-06-895T and *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts,* GAO-05-813.<br>*DHS updated information:* In March 2007, ICE provided updated information on its worksite enforcement program. Specifically, ICE reported that its worksite enforcement strategy includes (1) critical infrastructure protection, (2) criminal investigations of egregious employer violators, and (3) enhanced employer compliance and outreach through implementation of the ICE Mutual Agreement between Government and Employers. As part of its critical infrastructure protection efforts, ICE has undertaken enforcement actions to remove unauthorized workers from critical infrastructure sites, as those unauthorized workers may pose a threat to sensitive facilities. ICE has also engaged in criminal investigations targeting unscrupulous employers for significant criminal violations and has sought to prosecute employers' managers who knowingly hire unauthorized workers. ICE has also announced the first nine charter members of the ICE Mutual Agreement between Government and Employers, a program designed to build cooperative relationships between the federal government and businesses to strengthen hiring practices and reduce the employment of unauthorized workers. Through the program, ICE seeks to encourage industry compliance through enhanced employer training and education.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed a prioritized worksite enforcement strategy focused on critical infrastructure protection and egregious employers and has provided employers with a tool for enhanced training and education on compliance with laws prohibiting the employment of unauthorized workers. | Generally achieved |
| 8. Implement a prioritized worksite enforcement strategy to ensure that only authorized workers are employed | *GAO findings:* Our work has shown that DHS has faced challenges in implementing a prioritized worksite enforcement strategy. In August 2005 and June 2006 we reported that worksite enforcement was one of various immigration enforcement programs that competed for resources among ICE responsibilities and that worksite enforcement had been a relatively low priority. We reported that competing needs for resources and difficulties in proving that employers knowingly hired unauthorized workers hindered ICE's worksite enforcement efforts. In addition, ICE officials stated that the lack of sufficient detention space limited the effectiveness of worksite enforcement | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | efforts. We also noted that the availability and use of fraudulent documents made it difficult for ICE agents to prove that employers knowingly hired unauthorized workers. We reported that the number of notices of intent to fine issued to employers for improperly completing paperwork or knowingly hiring unauthorized workers generally declined between fiscal years 1999 and 2004. We also reported that the percentage of ICE agent work-years spent on worksite enforcement generally decreased between fiscal years 1999 and 2003. In addition, we reported that ICE lacked outcome goals and measures that hindered its ability to effectively assess the results of its worksite enforcement efforts. For example, we noted that until ICE fully develops outcome goals and measures, it may not be able to determine the extent to which its critical infrastructure protection efforts have resulted in the elimination of unauthorized workers' access to secure areas of critical infrastructure sites, one possible goal that ICE may use for its worksite enforcement program. For more information, see GAO-06-895T and GAO-05-813.<br>*DHS updated information:* In March 2007, ICE provided updated information on its worksite enforcement implementation efforts. ICE reported that during fiscal year 2006 it initiated about 1,200 worksite enforcement investigations, seized property and assets valued at approximately $1.7 million at the time of the initial enforcement action, and made 716 criminal arrests, a substantial increase over criminal arrests made in previous fiscal years. ICE reported that during fiscal year 2006 criminal fines, forfeitures, and payments in lieu of forfeiture yielded more than $2.5 million. ICE reported that it obtained criminal and civil judgments totaling $26.7 million as a result of its worksite enforcement efforts for the first quarter of fiscal year 2007. With regard to the third prong of ICE's worksite enforcement strategy—the ICE Mutual Agreement between Government and Employers—as of January 2007, ICE had nine employers as members.[b] One requirement for participation in this program is that member employers enroll in the Employment Eligibility Verification system, which allows participating employers to electronically verify the work authorization status of newly hired employees. ICE reported that it does not yet have systems in place to measure the effectiveness and success of its program. ICE reported that it does not collect data on program effectiveness because it would require the law enforcement agency to collect data from a wide range of agencies that are responsible for carrying out the specific law enforcement mission. ICE reported that it uses its law enforcement statistics (e.g., numbers of arrests, indictments, convictions, seizures, and forfeitures); consequences resulting from closed cases (e.g., indictments and convictions); and risk assessments to assess efficiency and effectiveness of its efforts. With regard to the consequences resulting from closed cases, ICE noted that a measure of success is if an investigation results in an indictment and a conviction. ICE reported that it measures the quality of cases and focuses its efforts on those cases that are the highest priority for protecting the United States. With regard to risk assessments, ICE reported that it conducts threat, vulnerability, and consequences assessments of customs and immigration systems to determine the greatest risks for exploitation by terrorists and other criminals and to determine the optimal application of resources to ensure the maximum contribution to national security and public safety. ICE reported that additional time is needed to afford its programs the opportunity to mature into an outcome-based system.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has taken actions to implement its worksite enforcement strategy and, among other things, has conducted more worksite enforcement investigations and made more criminal arrests in fiscal year 2006 in comparison to prior fiscal years. However, millions of unauthorized workers face little likelihood of confronting ICE worksite enforcements actions. Moreover, DHS did not provide us with evidence on | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | the extent to which its efforts have contributed to the achievement of ICE's desired outcomes for its worksite enforcement program and on the extent to which ICE has developed outcome goals and measures for its worksite enforcement program. We previously reported, without these goals and measures, it may be difficult for ICE to fully determine whether its worksite enforcement program is achieving its desired outcomes. With regard to the ICE Mutual Agreement between Government and Employers, the third prong of ICE's worksite enforcement strategy, we have previously identified weaknesses in one of the program's key requirements—participation in the Employment Eligibility Verification program. These weaknesses include the program's inability to identify document fraud, DHS delays in entering information into its databases, and some employer noncompliance with program. DHS has undertaken some efforts to address these weakness, but they would have to be fully addressed to help ensure the efficient and effective operation of an expanded program. | |
| 9. Develop a comprehensive strategy to interdict and prevent trafficking and smuggling of aliens into the United States | *GAO findings:* In prior work we reported that as of April 2005, ICE had not yet finalized a national strategy for combating alien smuggling.[c] For more information, see *Combating Alien Smuggling: Opportunities Exist to Improve the Federal Response,* GAO-05-305.<br>*DHS updated information:* In March 2007, ICE provided updated information on its efforts to develop a strategy to combat human smuggling and trafficking. For example, the Secure Border Initiative is a comprehensive, multiyear program established by the Secretary of Homeland Security to secure U.S. borders and reduce illegal immigration. The Secure Border Initiative includes DHS's efforts to identify and dismantle smuggling organizations. According to DHS, the Human Smuggling and Trafficking Center is an important component of DHS's strategy to combat alien smuggling. Additionally, ICE reported that, in 2006, it initiated its Trafficking in Persons Strategy to target criminal organizations and individuals engaged in human trafficking worldwide. The Trafficking in Persons Strategy focuses on building partnerships and collaboration with other DHS agencies, foreign governments, nongovernmental organizations, the Department of Justice Civil Rights Division, and federal, state, and local law enforcement.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has made progress toward developing a comprehensive strategy to interdict and prevent trafficking and smuggling of aliens into the United States by, for example, establishing the Human Smuggling and Trafficking Center and the Trafficking in Persons Strategy. | Generally achieved |
| 10. Implement a comprehensive strategy to interdict and prevent trafficking and smuggling of aliens into the United States | *GAO findings:* Our work has shown that DHS has faced challenges in implementing its antismuggling and trafficking mission.[d] In May 2005 we reported that ICE and CBP—two DHS components with antismuggling missions—signed a memorandum of understanding in November 2004 to address their respective roles and responsibilities, including provisions to ensure proper and timely sharing of information and intelligence. However, we reported that there was no mechanism in place for tracking the number and the results of referrals or leads made by CBP to ICE for investigation. Without such a mechanism, there may have been missed opportunities for identifying and developing cases on large or significant alien-smuggling organizations. CBP and ICE officials acknowledged that establishing a tracking mechanism would have benefits for both agencies. Such a mechanism would help ICE ensure that appropriate action is taken on the referrals. Also, CBP could continue to pursue certain leads if ICE—for lack of available resources or other reasons—could not take action on the referrals. For more information, see GAO-05-305. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | *DHS updated information:* In March 2007, DHS provided updated information on its antismuggling and trafficking efforts. With regard to smuggling, CBP established its Office of Alien Smuggling Interdiction to set guidelines for the development and maintenance of a program to address human smuggling incidents. This office is also intended to institutionalize information sharing within CBP on migrant smuggling, trafficking in persons, and clandestine terrorist travel. CBP noted that the office is still a work in progress, and CBP has established various goals and associated time frames for completing these goals. With regard to human trafficking, ICE reported that in fiscal year 2006 it opened nearly 300 human trafficking investigations and made about 180 arrests as a result of human trafficking investigations. ICE reported that since 2005 it has hosted or participated in training sessions on human trafficking and has collaborated with nongovernmental organizations that provide services to human trafficking victims. In addition, ICE reported on various initiatives to share information with CBP regarding human smuggling and trafficking. As previously discussed, ICE reported that it does not yet have systems in place to measure the effectiveness and success of its program. ICE reported that it does not collect data on program effectiveness because doing so would require the law enforcement agency to collect data from a wide range of agencies that are responsible for carrying out the specific law enforcement mission. ICE reported that it uses its law enforcement statistics (e.g., numbers of arrests, indictments, convictions, seizures, and forfeitures); consequences resulting from closed cases (e.g., indictments and convictions); and risk assessments to assess efficiency and effectiveness of its efforts. ICE reported that in May 2007, the ICE Offices of Investigations and International Affairs issued a joint memorandum to field offices providing guidance in accomplishing the component of the human trafficking strategy and requiring quarterly outreach reports and annual assessments. According to ICE, these quarterly reports and annual assessments will be used to monitor future progress in antitrafficking efforts.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. In prior work, we noted that effectiveness of a strategy for smuggling depends partly on having clearly defined roles and responsibilities for those agencies with antismuggling missions. CBP and ICE largely addressed this point in signing a memorandum of understanding and undertaking other information sharing initiatives. However, coordination between these two agencies and implementation of antismuggling efforts could be enhanced by development and use of a mechanism for sharing information. In addition, as part of its efforts to implement its antismuggling and trafficking strategy, DHS has identified the importance of performance evaluation but has not yet developed outcome goals and measures to assess the extent to which its efforts are achieving desired outcomes and has only recently initiated efforts to obtain quarterly reports and annual assessments from field offices. Until DHS has developed a mechanism to better share information among the responsible agencies and the ability to evaluate the outcomes of its efforts, DHS will not have a comprehensive strategy in place. In addition, although CBP has established goals for its Office of Alien Smuggling Interdiction, the majority of these goals have target time frames later than May 2007, or CBP noted that time frames are ongoing. | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 11. Develop a law enforcement strategy to combat criminal alien gangs in the United States and cross-border criminal activity | *GAO findings:* We have not completed work on DHS efforts to combat criminal alien gangs.[e]<br>*DHS updated information:* In March 2007, ICE provided updated information on its efforts to combat alien gangs. According to ICE, one of the goals of the Secure Border Initiative is to identify and remove immigration violators who are criminal aliens at large in the United States. ICE stated that it will use the additional resources in the proposed fiscal year 2008 budget to enhance ICE's anti-gang initiative—Operation Community Shield—and increase the number of transnational gang members that are identified, arrested, and removed from the United States. Operation Community Shield, a national law enforcement initiative, partners ICE with other federal, state, and local law enforcement. Additionally, ICE participates in the National Gang Targeting, Enforcement, and Coordination Center, a multi-agency national anti-gang enforcement targeting center, and in regular policy coordination meetings at the National Security Council concerning international organized crime. As a participant in the National Security Council Policy Coordination Committee meetings, ICE is assisting in the development of a strategy to combat transnational gangs in the United States, Mexico, and Central America.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has initiated various efforts, such as Operation Community Shield, in developing a strategy for combating criminal alien gangs. ICE has also worked with other agencies and groups to develop a strategy to combat alien gangs. | Generally achieved |
| 12. Implement a law enforcement strategy to combat criminal alien gangs in the United States and cross-border criminal activity | *GAO findings:* We have not completed work on DHS efforts to combat criminal alien gangs.[f]<br>*DHS updated information:* In March 2007, ICE provided updated information on its efforts to combat criminal alien gangs. Operation Community Shield was initiated by ICE in February 2005 to combat violent transnational street gangs and expanded to include all criminal and prison gangs. Under Operation Community Shield, ICE identifies violent gangs and develops intelligence on their membership; deters, disrupts, and dismantles gang operations by tracing and seizing their cash, weapons, and other assets; criminally prosecutes or removes gang members from the United States; partners with other law enforcement agencies at the federal, state and local levels to develop a force multiplier effect for gang investigations; and conducts outreach to boost public awareness about gangs. In March 2007, ICE reported that since its inception in February 2005, Operation Community Shield has resulted in the arrests of more than 4,000 gang members and associates. Additionally, ICE stated that it will provide staffing positions to identified high-threat gang areas based on the current transnational threat at the time the positions and funding are received. Given the mobility of transnational gangs, ICE will make a determination on the placement of resources in specific areas needing staffing based on tactical intelligence and other operational considerations. As previously discussed, ICE reported that it does not yet have systems in place to measure the effectiveness and success of its program, but uses its law enforcement statistics (e.g., numbers of arrests, indictments, convictions, seizures, and forfeitures); consequences resulting from closed cases (e.g., indictments and convictions); and risk assessments to assess efficiency and effectiveness of its efforts.<br>*Our assessment:* We cannot make an assessment of the extent to which DHS has generally achieved this performance expectation. We have not completed work related to DHS's effort to combat criminal alien gangs, and while DHS provided us with some information on its implementation efforts, we are unable to assess DHS's progress in achieving this performance expectation based on the information DHS provided. Specifically, DHS did not provide us with information that would clearly | No assessment made |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | enable us to assess the extent to which DHS's efforts to implement a strategy to combat alien gangs have resulted in desired outcomes. | |
| 13. Disrupt and dismantle mechanisms for money laundering and financial crimes | *GAO findings:* We have not completed work related to ICE's ability to disrupt and dismantle mechanisms for money laundering and financial crimes.[9]<br>*DHS updated information:* In March 2007, ICE provided updated information on its efforts to combat money laundering and financial crimes. With regard to a strategy for money laundering, ICE reported that it was a major contributor to the 2005 U.S. Money Laundering Threat Assessment produced by an interagency group to assess the progress that the United States had made in combating money laundering, evaluating the changing environment, and identifying areas that require further attention. ICE was also active in preparing the 2006 and 2007 National Money Laundering Strategies that addressed the findings and recommendations in the earlier report and set out goals, strategies, and specific actions for agencies to follow. The 2007 National Money Laundering Strategy noted that to measure the effectiveness of U.S. enforcement measures, ICE will compile investigative data. To support investigations with a potential nexus to terrorism and other financial crimes investigations, in July 2003, ICE launched Operation Cornerstone, an outreach program designed to identify and eliminate systemic vulnerabilities in financial systems that could be exploited by individuals, criminal organizations, and terrorists. ICE reported conducting more than 4,000 outreach presentations that have resulted in over 275 criminal investigations and $3 million seized since its establishment. With regard to bulk cash smuggling, ICE reported that the launch of Operation Firewall in August 2005, and its subsequent expansion in fiscal years 2006 and 2007, helped combat bulk cash smuggling. ICE reported that since its inception, Operation Firewall has resulted in the seizure of more than $76 million and the arrest of more than 200 suspects. ICE noted that the November 2004 establishment of Trade Transparency Units created cooperative international investigative efforts to identify and eliminate trade-based money laundering system, which supports the trafficking of drugs, people, and other contraband as well as terrorism. ICE also reported that it launched the Unlicensed Money Service Business/Informal Value Transfer System to prevent terrorists and other criminals from moving illicit funds through unlicensed money service businesses. Overall, in fiscal year 2006, ICE reported conducting nearly 4,000 financial investigations that resulted in more than 1,200 arrests and the seizure of more than $137 million in suspected illicit proceeds. As previously discussed, ICE reported that it does not yet have systems in place to prove that it has disrupted and dismantled mechanisms for money laundering and financial crimes. ICE reported that it uses its law enforcement statistics (e.g., numbers of arrests, indictments, convictions, seizures, and forfeitures); consequences resulting from closed cases (e.g., indictments and convictions); and risk assessments to assess efficiency and effectiveness of its efforts.<br>*Our assessment:* We cannot make an assessment of the extent to which DHS has generally achieved this performance expectation. We have not completed work related to DHS efforts to disrupt and dismantle mechanisms for money laundering and financial crimes. Although DHS provided us with some information on its implementation efforts, we are unable to assess DHS's progress in achieving this performance expectation based on the information DHS provided. Specifically, DHS did not provide us with information that would clearly enable us to assess the extent to which DHS's efforts to disrupt and dismantle mechanisms for money laundering and financial crimes have resulted in desired outcomes. | No assessment made |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 14. Develop a program to screen and respond to local law enforcement and community complaints about aliens who may be subject to removal | *GAO findings:* We have not completed work related to ICE programs for screening and responding to local law enforcement and community complaints about aliens who may be subject to removal.<br>*DHS updated information:* In March 2007, ICE provided updated information on its efforts to work with state and local law enforcement agencies. ICE reported that it in 2006 it initiated a pilot program, called the Law Enforcement Agency Response, in Phoenix, Arizona, to provide full-time response to local law enforcement agencies' requests for immigration-related assistance. As of March 2007, ICE reported that this program unit has received nearly 400 requests for assistance. ICE is studying the feasibility of continuing the pilot program and expanding it to other locations. In addition, ICE has established memoranda of agreement with 21 law enforcement agencies to provide training and assistance to state and local police and correctional personnel in the enforcement of federal immigration laws. ICE reported that as a result of these efforts, in fiscal year 2006 more than 6,000 individuals were arrested and, as of March 2007, more than 4,000 individuals have been arrested during fiscal year 2007 for violating misdemeanor and felony state and local laws. According to ICE, its Law Enforcement Support Center also provides information to law enforcement agencies relating to foreign nationals suspected of criminal activity and immigration status information of foreign nationals under arrest or investigation. Further, the Forensic Document Laboratory provides assistance to federal, state, tribal, local, and foreign authorities in making authenticity determinations of travel and identity documents.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed a number of programs to screen and respond to local law enforcement and community complaints about aliens who may be subject to removal. Additionally DHS has provided field guidance directing an enhanced response to state and local requests for information. | Generally achieved |
| 15. Develop staffing plans for hiring and allocating human capital resources to fulfill the agency's immigration enforcement mission | *GAO and DHS IG findings:* Since the transfer of responsibilities to DHS in March 2003, ICE has faced resource and financial management challenges that affected its ability to fully address all of its competing priorities. For example, ICE was faced with a hiring freeze in fiscal year 2004, which affected its ability to recruit, hire, and train personnel. Moreover, in June 2006 we reported that ICE did not yet have a formal risk management process for prioritizing and allocating its limited resources. Rather ICE primarily relied on the judgment of staff in major field offices in addition to national programs developed in headquarters. For more information, see *Information on Immigration Enforcement and Supervisory Promotions in the Department of Homeland Security's Immigration and Customs Enforcement and Customs and Border Protection*, GAO-06-751R.<br>*DHS updated information:* In March 2007, ICE provided updated information on its human capital functions. ICE reported that it has developed comprehensive staffing plans for all of the agency's critical positions in support of ICE's immigration enforcement mission and provided us with the operational assumptions underlying the staffing models. ICE also reported streamlining its hiring process and noted meeting all of its 2006 hiring goals. ICE reported (1) establishing preliminary guidance to provide ICE leadership and program managers with a framework for hiring and funding decisions and (2) implementing a workforce planning initiative to examine interdependencies and relationships among component programs. ICE stated that it has a hiring plan for supplemental, enhancement, and attrition hiring and that it is currently filling these positions. As of April 10, 2007, ICE reported that it has hired 1,213 employees in key occupations with 892 remaining for this fiscal year. ICE noted that Detention and Removal Operations is currently working toward hiring to its | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | authorized and funded level for positions of 6,762 and that approximately 5,222 positions are filled with 1,540 vacancies. Due to the number of vacancies, Detention and Removal Operations stated that it is striving to achieve a hiring goal that would ensure that at least 90 percent of its field and 85 percent of its headquarters vacancies are filled by the end of fiscal year 2007.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has provided information outlining its current staffing allocations and the operational basis of staffing models and has created initiatives to facilitate hiring and staffing. ICE staffing models are taken into consideration when requesting funds in the budget. | |
| 16. Provide training, including foreign language training, and equipment for all immigration enforcement personnel to fulfill the agency's mission | *GAO findings:* We have not completed work on DHS's provision of training for immigration enforcement personnel.<br>*DHS updated information:* In March and April 2007, ICE provided updated information on its training efforts. ICE reported that its ICE-D Basic Law Enforcement Training Program is an 18.5-week basic law enforcement training program that provides newly hired Detention and Removal Operations employees with entry-level training in law, tactical physical techniques, firearms, and operational training. ICE also reported that the Federal Law Enforcement Training Center has added a 5-week Spanish language immersion course that became part of the ICE-D program in April 2007. According to ICE, in November 2006 ICE offered a 4-hour instructor-led course on Alien Smuggling/Victims of Trafficking, but is in the process of developing a more balanced course that is not just focused on the southern border. ICE also offers other training courses. See Department of Homeland Security Office of the Inspector General, *A Review of Immigration and Customs Enforcement Discipline Procedures*, OIG-06-57 (Washington, D.C.: August 2006).<br>*Our assessment:* We cannot make an assessment of the extent to which DHS has generally achieved this performance expectation. We have not completed work related to DHS's effort to provide training and equipment to immigration enforcement personnel. While DHS provided us with some information on its training efforts, we are unable to assess DHS's progress in achieving this performance expectation based on the information DHS provided. Specifically, DHS did not provide us with information that would clearly enable us to assess the extent to which DHS has provided training, beyond basic training, for all immigration enforcement personnel. | No assessment made |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken a sufficient number of actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken a sufficient number of actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

[a] Under expedited removal, aliens apprehended within 100 miles of the border and within 14 days of entry who do not have documents, or who have false documents, can be removed from the United States without a hearing before an immigration judge.

[b] The other two prongs of ICE's worksite enforcement strategy are critical infrastructure protection and criminal investigations of egregious employer violators.

[c] In addition to DHS, other agencies, such as the Department of Justice, have a role to play in developing a strategy for antismuggling and trafficking. This performance expectation is focused on DHS's roles and responsibilities.

[d] In addition to DHS, other agencies, such as the Department of Justice, have a role to play antismuggling and trafficking efforts. This performance expectation is focused on DHS's roles and responsibilities.

[e] In addition to DHS, other agencies, such as the Department of Justice, have a role to play in developing a strategy for combating alien gangs. This performance expectation is focused on DHS's roles and responsibilities.

[f] In addition to DHS, other agencies, such as the Department of Justice, have a role to play in combating criminal alien gangs. This performance expectation is focused on DHS's roles and responsibilities.

[g] In addition to DHS, other agencies, such as the Department of Justice, have a role to play in disrupting and dismantling mechanisms for money laundering and financial crimes. This performance expectation is focused on DHS's roles and responsibilities.

## DHS Has Made Modest Progress in Providing Immigration Services

USCIS is the agency within DHS that is responsible for processing millions of immigration benefit applications received each year for various types of immigration benefits, determining whether applicants are eligible to receive immigration benefits, and detecting suspicious information and evidence to refer for fraud investigation and possible sanctioning by other DHS components or external agencies. USCIS processes applications for about 50 types of immigration benefits with a goal of ensuring that processing of benefits applications takes place within a 6 month time frame. USCIS has introduced new initiatives to modernize business practices and upgrade information technology infrastructure to transform its current, paper-based data systems into a digital processing resource to enhance customer service, prevent future backlogs of immigration benefit applications, and improve efficiency with expanded electronic filing.

As shown in table 20, we identified 14 performance expectations for DHS in the area of immigration services and found that overall DHS has made modest progress in meeting those expectations. Specifically, we found that DHS has generally achieved 5 performance expectations and has generally not achieved 9 others.

Table 20: Performance Expectations and Progress Made in Immigration Services

| Performance expectation | Assessment | | |
|---|---|---|---|
| | Generally achieved | Generally not achieved | No assessment made |
| 1. Eliminate the benefit application backlog and reduce application completion times to 6 months | | ✓ | |
| 2. Institute process and staffing reforms to improve application processes | ✓ | | |
| 3. Establish a timetable for reviewing the program rules, business processes, and procedures for immigration benefit applications | | ✓ | |
| 4. Institute a case management system to manage applications and provide management information | | ✓ | |
| 5. Develop new programs to prevent future backlogs from developing | | ✓ | |
| 6. Establish online access to status information about benefit applications | ✓ | | |
| 7. Establish online filing for benefit applications | | ✓ | |
| 8. Establish revised immigration application fees based on a comprehensive fee study | ✓ | | |
| 9. Capture biometric information on all benefits applicants | | ✓ | |
| 10. Implement an automated background check system to track and store all requests for applications | | ✓ | |
| 11. Communicate immigration-related information to other relevant agencies | ✓ | | |
| 12. Establish training programs to reduce fraud in the benefits process | | ✓ | |
| 13. Create an office to reduce immigration benefit fraud | ✓ | | |
| 14. Implement a fraud assessment program to reduce benefit fraud | | ✓ | |
| **Total** | **5** | **9** | **0** |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

Table 21 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of immigration services and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation's key elements (generally not achieved).

**Table 21: Performance Expectations and Assessment of DHS Progress in Immigration Services**

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Eliminate the benefit application backlog and reduce application completion times to 6 months | *GAO and DHS IG findings:* DHS has made significant progress in reducing the number of immigration benefit applications pending adjudication and has prioritized pending applications in a reasonable manner. However, USCIS cannot yet ensure that it has eliminated the backlog and reduced application completion time to 6 months primarily because (1) a large number of applications are still pending before the agency, many of which USCIS stated are of lower priority in its backlog elimination efforts, and (2) USCIS does not yet have a case management system for tracking applications it receives to determine whether applications are processed within 6 months of receipt. In addition, USCIS has yet to demonstrate that it has overcome long-standing technology problems. With respect to an immigration benefit application, the term backlog, as defined by statute, means the period of time in excess of 180 days (6 months) that such application has been pending before USCIS. USCIS, using its operational definition of backlog, measures the volume of its backlog as the number of applications pending before the agency in excess of the number of applications received in the most recent 6 months. USCIS then subtracts from this number all applications pending where either benefits would not be immediately available even if the applications were granted or further adjudication of the application depends on action by another agency or the applicant.<br>USCIS stated that by consistently completing more applications than are filed each month, the agency should gradually reduce its pending workload of applications to a level at which it can complete all incoming applications within the workload targets established for each application type. Eventually, according to the agency's backlog elimination plan, as long as USCIS is processing more applications than it is receiving, there should be no backlog. However, we reported that under USCIS's definition of backlog, the agency cannot guarantee that every applicant requesting a benefit will receive a decision within 6 months of filing. Moreover, although USCIS's data showed a significant decrease in the backlog from January 2004 through June 2005, we reported that the sharp drop in the backlog was due to USCIS's decision in July 2004 to remove from its backlog count those 1.15 million cases for which an immigration visa was not immediately available and a benefit therefore could not be provided. In September 2005, the DHS IG noted that removal of some applications from the backlog, as well as other backlog reduction efforts such as the hiring of temporary staff, may have benefited the agency in the short-term. However, the DHS IG reported that these actions would not resolve the long-standing processing and information technology problems that contributed to the backlog in the first place and that, until these problems were addressed, USCIS would not be able to apply its resources to meet mission and customer needs effectively.<br>In our previous work, we noted that USCIS's automated systems were not complete and reliable enough to determine how long it actually takes to process specific benefit applications or to determine the exact size of its backlog. USCIS has identified requirements for transforming its information technology systems to address deficiencies in its capabilities, but these transformation efforts have not yet been fully developed or implemented. We reported that until USCIS develops this capability, it cannot assure Congress that it has successfully eliminated the backlog, and it will not be able to provide accurate information about the actual number of applications that have been pending in excess of 180 days or the actual amount of time they have been pending. For more information, see *Immigration Benefits: Improvements Needed to Address Backlogs and Ensure Quality of Adjudications,* GAO-06-20. Also, see Department of | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | Homeland Security Office of Inspector General, *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology,* OIG-07-11 (Washington, D.C.: November 2006) and *USCIS Faces Challenges in Modernizing Information Technology,* OIG-05-41 (Washington, D.C.: September 2005).<br>*DHS updated information:* In March through June 2007, DHS provided updated information on its backlog. In January 2004, USCIS had approximately 3.8 million applications backlogged pending adjudication, including applications that, according to USCIS, if granted would not provide the applicant or petitioner with an immediate immigration benefit or were pending as a result of delays outside of USCIS's control. Based on an analysis of data provided in USCIS's Backlog Elimination Plan Update for the fourth quarter of fiscal year 2006, as of September 2006, USCIS had a total of about 1.0 million backlogged applications, including applications that, according to USCIS, if granted would not provide the applicant or petitioner with an immediate immigration benefit or were pending as a result of delays outside of USCIS's control. As a subset of this 1.0 million, USCIS reported that the backlog under its control was less then 10,000. Specifically, for each application type, USCIS removed from the calculated backlog the total number of pending applications that, even if the application were granted, the ultimate benefit sought would not be immediately available due to annual numerical caps set by statute. As reported in the USCIS Backlog Elimination Plan updates, certain applications and petitions were removed from the backlog count because (1) the benefit was not immediately available to the applicant or beneficiary; (2) USCIS was waiting for applicants or petitioners to respond to requests for information; (3) applicants were afforded the opportunity to retake naturalization tests; or (4) USCIS was waiting for actions from outside federal agencies, such as Federal Bureau of Investigation name checks. USCIS has previously acknowledged that there may be some applications that have been pending more than 6 months and reported to us that the agency cannot determine the precise composition of the total applications pending adjudication as of September 2006 because such data are not available for all applications within USCIS.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. USCIS has made significant progress in reducing the number of applications pending adjudication and processing times for adjudicating applications. However, USCIS's method of calculating its backlog leaves the possibility of individual applications pending for longer than 6 months, so long as in the aggregate the number of pending applications on any given date does not exceed the number received in the previous 6 months. USCIS has acknowledged that some applications received in fiscal years 2005 and 2004, or even earlier, may still be pending. Moreover, USCIS removed from its backlog calculation any pending applications for which a benefit would not be immediately available, even if the application were granted, or that were awaiting action outside of USCIS. While giving such applications lower priority is a reasonable approach to backlog reduction and is useful for workload analysis, those applications—1 million as of September 2006—are still awaiting adjudication. For example, about 750,000 of these applications are those for which a benefit would not be immediately available even if granted, according to USCIS. Adjudicating these applications would let applicants or their beneficiaries know their eligibility for benefits, however, and could prevent future delays if large numbers of these benefits suddenly became immediately available due to a statutory increase in the caps, as happened when a 2005 law eliminated the annual cap on asylum beneficiaries. Additionally, DHS's current data systems cannot produce backlog information based on the date of the filing of a benefit application, which contributes to USCIS's difficulty in measuring its backlog consistent with the statutory definition, upon which the performance expectation is in part based, and in providing information on whether it is processing applications within 6 months of receipt. USCIS has not yet demonstrated that it has overcome long-standing technology problems which, according to the DHS IG, contributed to the backlog in the first place. Without information on whether individual applications have been pending for more than 6 months, we cannot verify that USCIS has eliminated its backlog and reduced application completion time to 6 months. | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 2. Institute process and staffing reforms to improve application processes | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. We reported that in fiscal year 2002 USCIS committed about 70 percent of its backlog reduction funds to employing about 1,100 temporary adjudicator staff and authorizing overtime. In May 2005, USCIS finalized a staffing allocation model to address how many and where staff were needed to better match projected workloads. On the basis of this model, USCIS determined it had to retain the temporary adjudicators currently on hand (about 1,100) through the end of fiscal year 2006 and fill vacancies to increase its level of permanent adjudicator staff by 27 percent (about 460) to maintain productivity and prevent future backlogs through fiscal year 2007. Additionally, USCIS's staffing model addressed how many and where staff were needed to better match projected workloads. USCIS officials said that the need for future staffing adjustments could be offset by future efficiencies gained during its transition to more robust information technology capabilities. We reported that reflection in its planning processes and documents of expected gains as a result of new technologies should improve USCIS's ability to make strategic staffing decisions. In addition, we reported that USCIS issued guidance and regulations to streamline processes, including clarifying guidance to adjudicators about requests for additional evidence and notices of intent to deny, and establishing greater flexibility in setting the length of validity of the employment authorization document. For more information, see GAO-06-20. | Generally achieved |
| 3. Establish a timetable for reviewing the program rules, business processes, and procedures for immigration benefit applications | *GAO and DHS IG findings:* DHS has not yet established a timetable for reviewing program rules, processes, and procedures for immigration benefits applications. In November 2006, the DHS IG reported that USCIS had undertaken a structured approach to address process challenges through its business transformation program and established cross-functional teams with dedicated management participation and generated several strategic level plans to provide a business-centric vision and guidance for implementing technical solutions. The DHS IG reported that the accomplishments to date were steps in the right direction for both business and information technology modernization, but that USCIS remained entrenched in a cycle of continual planning, with limited progress toward achieving its long-term transformation goals. Obtaining the funding needed to support implementation of the business transformation program was a continual concern. The DHS IG reported that establishing a clearly defined transformation strategy, including the funding plans, goals, and performance measures needed to manage its execution, is fundamental. Linking information technology objectives to this transformation strategy and ensuring sufficient internal and external stakeholder involvement in information technology and process improvement initiatives also would be key. The DHS IG reported that until USCIS addresses these issues, it would not be in a position to either effectively manage existing workloads or handle the potentially dramatic increase in immigration benefits processing workloads that could result from proposed immigration reform legislation. For more information, see Department of Homeland Security Office of Inspector General, *U.S. Citizenship and Immigration Services' Progress in Modernizing Information Technology,* OIG-07-11 (Washington, D.C.: November 2006).<br>*DHS updated information:* According to updated information provided by USCIS in March and April 2007, the USCIS Transformation Program Office will prepare its detailed timetable for reviewing program rules, business processes, and procedures for each benefit category once it receives and awards the contract for information technology services. USCIS reported analyzing over 50 existing transactions and grouped them into lines of business—the adjudication of citizenship benefit applications, immigrant benefit applications, humanitarian benefit applications, and non-immigrant benefit applications. USCIS has incorporated a timetable for incrementally implementing each of the lines of business in its transformation expenditure plan. USCIS plans to transform benefit adjudication for citizenship benefits by October 2008; immigrant benefits by October 2010; humanitarian benefits by October 2011; and non-immigrant benefits by October 2012. USCIS reported that the Transformation Spend Plan has been approved by the Office of Management and the Budget and that the plan's transmittal to Congress should occur shortly. According to the tentative schedule, USCIS plans to transform its paper-based process into an | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | electronic end-to-end adjudicative process.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. USCIS has made progress in meeting this performance expectation, but has not yet established a detailed timetable for reviewing program rules, processes, and procedures for immigration benefits applications. USCIS officials noted that the agency will prepare its detailed timetable for reviewing program rules, business processes, and procedures for each benefit category once it receives and awards the contract for information technology services. Until USCIS establishes such a timetable, it has not yet achieved this performance expectation. | |
| 4. Institute a case management system to manage applications and provide management information | *GAO findings:* DHS has not yet instituted a case management system for managing applications and providing management information. In November 2005, we reported that USCIS cannot readily determine the number of applications that have been pending for more than 6 months from the data management systems it is currently using to manage its backlog elimination efforts. However, USCIS has identified the technology improvements necessary to develop this capability. Since fiscal year 2002, the agency has invested about 2 percent ($10.5 million) of its funds allocated for backlog elimination for technology improvements. We reported that among the critical elements of USCIS's planned technology modernization efforts was a new case management system that should provide the agency with the capability to produce management reports on the age of all pending benefit applications. We reported that an integrated case management system is a tool that will be used by USCIS staff in processing benefits and adjudicating cases. USCIS reported that system development began during fiscal year 2006 as part of the agency's transformation efforts. In November 2005, we reported that USCIS was assembling the system requirements and conducting surveys of industry best practices. In addition, USCIS reviewed a cost-benefit analysis to evaluate alternative implementation strategies for the new integrated case management system. USCIS anticipated that its current case management systems would be decommissioned by fiscal year 2011. We reported that USCIS did not expect these systems to be fully deployed before fiscal year 2010. For more information, see GAO-06-20.<br>*DHS updated information:* According to USCIS, a case management system to manage applications and provide management information will be incorporated in the Secure Information Management Service, for which the first increment pilot was deployed in July 2007. This increment will include forms related to USCIS's citizenship function. Three additional increments will address the functions of immigrant, asylum/refugee, and nonimmigrant. USCIS noted that development of its case management system is tied to transformation that began in fiscal year 2006.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although USCIS is planning to pilot the first phase of its Secure Information Management Service, USCIS does not yet have a case management system that provides reliable information on its application processing and backlog. | Generally not achieved |
| 5. Develop new programs to prevent future backlogs from developing | *GAO findings:* DHS has taken actions to examine and test new programs to prevent future backlogs, but these programs are still in the pilot stages. In 2005 we reported that in response to recommendations made in the USCIS Ombudsman's 2004 annual report, USCIS conducted a number of pilot projects designed to reduce benefit application processing times and was considering adopting several practices it determined to be successful. We reported that the agency studied the processing of two types of applications during the pilots: (1) applications to replace permanent resident cards (form I-90) and (2) applications to register permanent residence or adjust status (form I-485). First, during the period March 2004 through November 2004, USCIS conducted a pilot program designed to reduce processing time for applications for permanent resident cards. The pilot, conducted in the Los Angeles area, allowed for electronically filed permanent resident cards to be processed at application support centers, where applicants have their initial contact with the agency and have their photographs and fingerprints taken. During the pilot, average processing times were reduced from over 8 months | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | to about 2 weeks. USCIS's Performance Management Division recommended that USCIS implement the pilot nationwide. Second, beginning in March 2004 and May 2004 respectively, USCIS conducted pilot programs in the New York and Dallas district offices that focused on testing new processes for adjudicating family-based applications for adjustments of status within 90 days. Each sought to streamline and accelerate application processing by shifting aspects of processing responsibility from the National Benefits Center, a central processing hub for certain benefit applications, to the district offices. Using elements of processes tested in the Dallas and New York pilot projects, USCIS has implemented up-front processing at three district offices—San Diego, San Antonio, and Buffalo—that did not have a backlog of adjustment of status applications when implemented. USCIS anticipates expanding the number of offices on a quarterly basis as they become current in their processing so that applicants with pending applications are not disadvantaged. The pilot in Dallas will also continue as long as USCIS determines that additional information may be gleaned and until the district office becomes current in processing applications. In March 2004, a third adjustment of status pilot for employment-based applications was implemented at the California service center. The focus was to adjudicate within 75 days petitions for immigrant workers with advanced degrees concurrently with the associated applications for adjustment of status. Ultimately, USCIS deemed the pilot inefficient and adverse to the service center backlog elimination goals because resources were diverted from addressing backlogged cases. For more information, see GAO-06-20.<br>*DHS updated information:* According to information provided by DHS in March, April, and May 2007, in September of 2006, USCIS expanded its District Office Rapid Adjudication Pilot program by extending that program in Dallas, the office of origin, and by including field offices located in El Paso and Oklahoma City. USCIS noted that for applicants within the jurisdiction of these offices, the pilot program makes it mandatory that adjustment of status applications be filed in person rather than by mail, after the applicant has scheduled an appointment using InfoPass. According to USCIS, the pilot is slated to run through September 21, 2007. Additionally, USCIS stated that it is monitoring the adjustment of status workflow in three identified offices, Buffalo, San Antonio, and San Diego, which are currently within a 90-day processing time frame. Under the "90-Day Office" process, processing is initiated on the application at the National Benefits Center. To date, USCIS noted that it has not captured sufficient statistical data to assess the effects of expanding the Dallas pilot to El Paso and Oklahoma City. Moreover, it has yet been able to assess whether the process in the Dallas pilot or the "90-Day Office" process is more likely to result in better customer service, administrative efficiency, and national security. USCIS issued a final rule in May 2007 to adjust the Immigration and Naturalization Benefit Application and Petition Schedule. According to USCIS, this rule will help ensure that the agency has the resources necessary to prevent backlogs from developing by providing a stable source of revenue to support staff and technology to meet USCIS's goal of at least a 20 percent reduction in processing times by the end of fiscal year 2009.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although USCIS has explored reducing processing times through a number of programs, these programs are still in the pilot stages. In some cases, USCIS ended the pilot programs because they were inefficient or did not meet program goals. In other cases, USCIS has not yet fully assessed the results of its pilot programs to determine the extent to which the programs could be implemented on a national basis. Moreover, USCIS has not yet demonstrated that it has addressed its long-standing technology challenges, which have contributed to backlog development. In addition, USCIS reported that its revisions to the Immigration and Naturalization Benefit Application and Petition Schedule will help it ensure that future backlogs do not develop. However, at the time of this review, the extent to which these revisions will help to prevent the development of future backlogs is unknown. | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 6. Establish online access to status information about benefit applications | *GAO findings and assessment:* DHS has established online access to status information about benefits applications. In June 2005, we reported that private attorneys, paralegals, and other representatives can use the USCIS Internet Web site to check the status of their clients' immigration cases using a USCIS receipt number. Under the system, USCIS also notifies the representatives via e-mail when a case status changes; for example, when actions are taken, such as the approval or denial of an application. As of April 2005, over 300,000 customers, attorneys, and other representatives had used this system. For more information, see *Immigration Services: Better Contracting Practices Needed at Call Centers,* GAO-05-526. | Generally achieved |
| 7. Establish online filing for benefit applications | *GAO findings:* On November 1, 2006, USCIS announced a new Web portal to serve as a "one-stop shop" for all information about U.S. immigration and citizenship. According to DHS, the new site should facilitate downloading of petitions and applications, filing applications electronically, and signing up online for appointments.<br>*DHS updated information:* In March and April 2007, DHS provided updated information on its efforts to establish online filing for benefit applications. In fiscal year 2006, USCIS reported that of the 5,953,490 forms filed, a total of 350,838 were filed online. According to updated information provided by DHS in April 2007, eight forms are available online for e-filing, and other forms are available on the USCIS Web site for downloading, completing, and mailing to the appropriate Service Center. According to USCIS, the Secure Information Management Service, with the citizenship increment released in July 2007, will serve as the foundation for the paperless, account-based case processing environment, and subsequent releases of the immigration, asylum/refugee, and nonimmigration increments will result in additional online e-filing capabilities. In addition, USCIS stated that while it may be feasible to automate additional forms and make them available electronically, USCIS transformation will fundamentally reengineer e-filing, increase data integrity, and increase operational efficiency.<br>*Our assessment:* Until USCIS expands its online filing capabilities and further defines requirements and capabilities and implements those capabilities through its Secure Information Management Service, we conclude that DHS has generally not achieved this performance expectation. Although DHS has established online filing for eight types of applications, there are other types of applications for which online filing is not yet available. Moreover, USCIS plans to expand its online filing capabilities through its Secure Information Management Service, but this service is still in the development stages and has not yet been implemented. | Generally not achieved |
| 8. Establish revised immigration application fees based on a comprehensive study | *GAO findings:* USCIS issued a proposed rule to adjust immigration benefit fees and issued the final rule in May 2007. As required under the Homeland Security Act of 2002, we reviewed the USCIS's funding to determine whether in the absence of appropriated funds USCIS was likely to derive sufficient funds from fees to carry out its functions. In January 2004, we concluded that USCIS fees were not sufficient to fully fund USCIS's operations, in part because (1) the fee schedule was based on an outdated fee study that did not include all costs of USCIS's operations and (2) costs had increased since that study was completed due to an additional processing requirement and other actions. We reported that although fees were not sufficient, there were insufficient data to determine the full extent of the shortfall. A fundamental problem was that USCIS has not had a system to track the status of each application as it moves through the process. Accordingly, USCIS did not have information on the extent to which work on applications in process remained to be finished. In addition, USCIS did not know the current cost of each step to process each application. The effect was that USCIS knew neither the cost to process new applications nor the cost to complete pending applications. Further because DHS was still determining how administrative and overhead functions would be carried out and the related costs allocated, USCIS did not know what future administrative and overhead costs would be. For the 3-year period from fiscal year 2001 through 2003, USCIS reported operating costs exceeded available fees by almost $460 million, thus creating the need for appropriated funds. USCIS projected that this situation would remain in fiscal year 2004. We reported that absent actions to increase fees, reduce processing costs and times, or both, as well as to | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | improve the timeliness and completeness of fee schedule updates, USCIS would continue to need appropriated funds to avoid even greater increases in the backlog of pending applications. We recommended that in order to determine the cost to process new and pending applications, USCIS should perform a comprehensive fee study to determine the cost to process new immigration applications and determine the cost to eliminate the backlog of pending applications. For more information, see *Immigration Application Fees: Current Fees Are Not Sufficient to Fund U.S. Citizenship and Immigration Services' Operations,* GAO-04-309R.<br>*DHS updated information:* On February 1, 2007, USCIS issued a Proposed Rule for the Adjustment of the Immigration and Naturalization Benefit Applications and Petition Fee Schedule and issued the final rule in May 2007. Based on a 2004 GAO recommendation, USCIS conducted a comprehensive review of its resources and activities for the first time in 10 years, employing the Activity Based Costing methodology to determine the full costs of immigration benefit applications and in which USCIS fees are based on the complexity of the work. In updated information provided by DHS in March and April 2007, USCIS stated that the new fee structure ensures appropriate funding to meet customer service needs and national security requirements and modernizes an outdated business infrastructure. According to DHS, the fiscal year 2008 President's budget reflects that 99 percent of USCIS funding would be derived from fee collections. The remaining 1 percent, $30 million, is requested as an appropriation to support the Employment Eligibility Verification program. According to USCIS, a number of problems caused the present day funding gap, including (1) the failure of fees to reflect the actual cost of doing business, (2) the loss of significant appropriated funding for backlog reduction, (3) the need for payment of additional fees because of processing delays, (4) reliance on money from temporary programs to fund operating costs, (5) reallocation of funds from their intended purpose to cover base operations, and (6) insufficient funds to provide for additional, costly security requirements. USCIS indicated that additional funding was necessary to enhance the security and integrity of the immigration system, improve service delivery, and modernize business infrastructure.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. In following up on our prior recommendations, we found that USCIS has conducted a comprehensive review of its resources and activities and determined that the current fees did not reflect current processes or recover the full cost of services being provided. USCIS employed an activity-based costing methodology to determine the full costs of immigration benefit applications. As a result of its comprehensive fee review, USCIS published a proposed rule in February 2007 in the Federal Register and a final rule in May 2007 to increase the immigration and naturalization benefit application fees. | |
| 9. Capture biometric information on all benefits applicants | *GAO and DHS IG findings:* DHS does not yet have the capabilities in place to capture and store biometric information on all benefits applicants. In 2006 we reported that USCIS was developing various systems for capturing and storing biometric information including the Biometric Storage System, which would allow USCIS to store biometrics information for verification of identity and for future form submissions. USCIS planned to expand biometric storage capacity to allow storage of biometric information for all USCIS customers, allowing information to be resubmitted for subsequent security checks. The system would capture 10 prints for Federal Bureau of Investigation fingerprint checks and image sets (photograph, press-prints, and signatures). Senior officials told the DHS IG that USCIS's use of biometrics had been constrained by the capacity of application support centers to collect the data. In addition, the DHS IG reported in November 2005 that USCIS collected photographs with many applications but did not have a system for automated, facial recognition screening. For more information, see GAO-06-20. Also, see Department of Homeland Security Office of Inspector General, *A Review of U.S. Citizenship and Immigration Services' Alien Security Checks,* OIG-06-06 (Washington, D.C.: November 2005).<br>*DHS updated information:* According to DHS officials, the Biometric Storage System is in the | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | design phase. According to the Biometric Storage System Project Management Plan, the system is intended to facilitate the deterrence, detection, and pursuit of immigration benefit fraud and promote identification and communication of immigration-related information to partners in support of the DHS Strategic Plan. In developing the system, USCIS plans to leverage existing capabilities already being developed by other components in the immigration and border management enterprise. USCIS plans to share Biometric Storage System data with the US-VISIT biometric repository called IDENT. This should enable data sharing and provide USCIS information about applicants with a record in IDENT. USCIS estimated that the first phase of Biometric Storage System, which will replace existing outdated biometrics infrastructure with a foundation for the new system, would begin in the first quarter of fiscal year 2008. At that time, USCIS plans to have access to limited biometrics data available to the intra-agency community—ICE, CBP, and USCIS—on a view-only basis. USCIS reported that although the Biometric Storage System is not yet in place, the agency shares biometric information with US-VISIT and the Federal Bureau of Investigation, for example.<br>*Our assessment:* Until the Biometric Storage System is more fully developed and implemented, we conclude that DHS has generally not achieved this performance expectation. DHS has not yet deployed its Biometric Storage System, but plans to implement the first phase of the system in 2008. | |
| 10. Implement an automated background check system to track and store all requests for applications | *GAO findings:* DHS has not yet implemented an automated background check system to track and store all requests for applications. In 2006 we reported that USCIS's Background Check Service system automated and managed the submission of all security checks including name and fingerprints from the Federal Bureau of Investigation and the Interagency Border Inspection System. We noted that the Background Check Service system was intended to track and store security check responses in a centralized system and that USCIS was preparing to initiate the testing and implementation phase, but USCIS had to first select a hosting and production facility for the system. For more information, see GAO-06-20.<br>*DHS updated information:* In March, April, and June 2007, USCIS provided us with updated information on its efforts to develop and implement its Background Check Service. According to USCIS, the schedule for deploying the Background Check Service has changed from May 2007 to December 2007 because USCIS moved the Background Check Service to a new location and encountered problems at the new center. According to USCIS, there were several firewall issues and other communication problems, but the problems are being worked on by the contractor.<br>*Our assessment:* Until DHS more fully develops and implements its Background Check Service, we conclude that DHS has generally not achieved this performance expectation. DHS has worked toward deployment of the first phase of its Background Check Service, but has pushed back its target time frame for deploying the first phase until December 2007. | Generally not achieved |
| 11. Communicate immigration related information to other relevant agencies | *GAO findings:* DHS has taken some actions to share immigration information for enforcement and fraud prevention purposes. In 2006 we reported that USCIS had three major projects under way to improve its ability to receive and share data within the agency as well as with other agencies as part of its information technology transformation. First, the data layer/repository project was intended to present users with a consolidated system to access information from 63 USCIS systems rather than the situation where users had to log onto separate systems to obtain data. This capability would be available to adjudicators and, eventually, to external users. Second, the software updates project was intended to upgrade, among other things, USCIS's desktop and software capabilities, USCIS's servers and network, and USCIS's capability to support the new electronic processes. Third, the e-adjudication pilot project was intended to allow paperless (electronic) adjudication for certain immigration forms. USCIS could not provide a completion date for the data layer and e-adjudication pilots due, in part, to uncertainty regarding future funding. USCIS expected to complete full implementation for its information technology transformation by fiscal year 2010. With regard to US-VISIT, we reported that the program intended to collect, maintain, and share information on certain foreign nationals who | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | enter and exit the United States and facilitate information sharing and coordination within the immigration and border management community. For more information, see *Taxpayer Information: Options Exist to Enable Data Sharing between IRS and USCIS but Each Presents Challenges,* GAO-06-100 and GAO-06-20.<br>*DHS updated information:* According to updated information provided by DHS in March, April, and May 2007, in fiscal year 2006 USCIS launched the Integrated Digitization Document Management Program to convert existing paper-based A-files and related documents into a digitized format; ensure that data are accurately captured electronically from paper A files; and provide storage, discovery, and electronic delivery of digitized files. USCIS stated that the last function was released in June 2007. USCIS has entered into a number of memoranda of understanding that outline agreements on immigration-related information sharing with other federal agencies and foreign governments. In addition, immigration information is shared though others programs, such as US-VISIT. US-VISIT, for example, provides for the sharing of biometric and biographic-related information between DHS components, and the Departments of Justice and State. USCIS, CBP, and ICE have also entered into memoranda of understanding with other federal agencies and foreign governments to enhance information sharing.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has taken some actions to develop and launch systems to facilitate information sharing with other agencies, such as by allowing for the electronic delivery of files and information. Moreover, USCIS has completed memoranda of understanding with other agencies. | |
| 12. Establish training programs to reduce fraud in the benefits process | *GAO findings:* DHS has made progress in establishing training programs to reduce fraud in the benefits process, but more work remains. In 2006 we reported that adjudicators at USCIS service centers and district offices that we visited received some fraud-related information or training subsequent to their initial hire. We reported that USCIS initial adjudicator training provided approximately 4 hours of fraud-related training that focused primarily on detecting fraudulent documents. However, USCIS headquarters officials responsible for field operations told us that there was no standard training regarding fraud trends and that fraud-related training varied across field offices. Our interviews indicated that the frequency and method for distributing ongoing information about fraud detection was not uniform across the service centers and district offices we visited. For more information, see *Immigration Benefits: Additional Controls and a Sanctions Strategy Could Enhance DHS's Ability to Control Benefit Fraud,* GAO-06-259.<br>*DHS updated information:* In March and April 2007, DHS provided updated information outlining its training programs to reduce fraud in the benefits process. With regard to adjudication officers, the Office of Fraud Detection and National Security has created an hour anti-fraud module that is provided to adjudicators attending immigration officer basic training, journeyman Immigration Officer training, and supervisory adjudications training. USCIS has also developed training for specific areas with a past history of fraud. For example, USCIS has provided Religious Worker anti-fraud training to 145 officers at the California Service Center where adjudication of religious worker petitions is centralized. With regard to Office of Fraud Detection and National Security Officers, during a basic 3-week national security and anti-fraud course at the Federal Law Enforcement Training Center, instruction is provided to these officers on such areas as Fraud Detection and National Security anti-fraud standard operating procedures, practical training on USCIS and other government systems, interviewing techniques, national security reporting, Headquarters Fraud Detection and National Security intelligence processes, legal issues, and report writing. Additionally, all Immigration Officers and Intelligence Research Specialists must attend the Fraud Detection and National Security Data System training, which serves as the case management system for all fraud and national security related work conducted by the Office of Fraud Detection and National Security, as part of the basic 3-week course and will continue to be provided ongoing training as systems evolve through the use of formal correspondence, informal conference calls, e-newsletters.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | expectation. USCIS has initiated a number training programs focused on detecting fraud in the benefits process. However, the intent of this performance expectation is not only that DHS has anti-fraud training programs, but also that these programs are delivered to individuals according to their roles and responsibilities for adjudicating applications. DHS did not provide us with evidence on the extent to which it has taken actions to ensure that its anti-fraud training courses have been distributed and implemented appropriately across all field offices, a key concern we identified in our prior work. In addition, DHS did not provide us with evidence that it has taken actions to ensure that all staff receive the anti-fraud training appropriate to their roles and responsibilities in adjudicating certain types of applications. | |
| 13. Create an office to reduce immigration benefit fraud | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. USCIS established the Fraud Detection and National Security office to enhance its fraud control efforts by serving as its focal point for addressing immigration benefit fraud. Established in 2003, Fraud Detection and National Security is intended to combat fraud and foster a positive control environment by pursuing objectives to develop, coordinate, and lead the national antifraud operations for USCIS; oversee and enhance policies and procedures pertaining to the enforcement of law enforcement background checks on those applying for immigration benefits; identify and evaluate vulnerabilities in the various policies, practices, and procedures that threaten the legal immigration process; recommend solutions and internal controls to address these vulnerabilities; and act as the primary USCIS conduit and liaison with ICE, CBP, and other members of the law enforcement and intelligence community. For more information, see GAO-06-259. | Generally achieved |
| 14. Implement a fraud assessment program to reduce benefit fraud | *GAO findings:* DHS has taken steps to implement a fraud assessment program, but much more work remains. In 2006 we reported that the Office of Fraud Detection and National Security, established in 2003, outlined a strategy for detecting immigration benefit fraud, and undertook two assessments in a series of fraud assessments to identify the extent and nature of fraud for certain immigration benefits. A complimentary effort is USCIS's plan to develop automated fraud analysis tools. USCIS has hired a contractor to develop the Fraud Detection and National Security, an automated capability to screen incoming applications against known fraud indicators, such as multiple applications received from the same person. According to the Office of Fraud Detection and National Security, it planned to deploy an initial data analysis capability by the third quarter of fiscal year 2006 and release additional data analyses capabilities at later dates but could not predict when these latter capabilities would be achieved. However, according to a Fraud Detection and National Security operations manager, the near and midterm plans were not aimed at providing a full data-mining capability. In the long term, USCIS planned to integrate these data analyses tools for fraud detection into a new application management system being developed as part of USCIS's efforts to transform its business processes for adjudicating immigration benefits, which includes developing the information technology needed to support these business processes. Also, in the long term, according to the Fraud Detection and National Security Office Director, a new USCIS application management system would ideally include fraud filters to screen applications and remove suspicious applications from the processing stream before they are seen by adjudicators. For more information, see GAO-06-259.<br>*DHS updated information:* According to USCIS, the purpose of the benefit fraud assessment is to use statistically valid methods to determine the amount, percentage, and type of fraud in benefit applications to aid USCIS in its efforts to develop anti-fraud strategies, establish priorities for planning purposes, and identify fraud patterns and linkages for referral to ICE. In updated information provided by USCIS in April 2007, USCIS reported that it has completed benefit fraud assessments for the I-140 Immigrant Petition for Alien Workers, I-90 Application to Replace a Permanent Resident Card, and Religious Worker applications. USCIS reported that it is analyzing data from other assessments of the I-129 H1B Employment-based, I-130 Marriage-based, I-130 Yemeni-specific Family-based, and 1-589 Asylum applications and expect final reports on these assessments to be issued by the end of fiscal year 2007. USCIS also reported that it is conducting an assessment for I-129 L-1A Employment-based application. USCIS | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
|  | reported that as a result of these assessments, it now has baseline data and can focus on developing a more comprehensive benefit fraud assessment strategy. In fiscal year 2008, USCIS intends to issue a roadmap outlining the visa categories for which it will conduct benefit fraud assessments in the future. In addition, USCIS officials stated that development work for the Fraud Detection and National Security Program Data Systems' initial analytical capabilities was completed in the first quarter of fiscal year 2007. USCIS indicated that development delays for the initial analytical capabilities were encountered due to budgetary, contractual, and performance issues. Full implementation of the initial capability was delayed until the second quarter of fiscal year 2007 due to hardware acquisition issues. According to USCIS, procurement activities are underway to award the next development contract with a plan that includes a contract award in early third quarter of fiscal year 2007 with the implementation of follow-on analytical capabilities early in the first quarter of fiscal year 2008. USCIS stated that this procurement was briefly delayed due to an evaluation of another case management software application. A final decision was made in February 2007 to move forward with the development of Fraud Detection and National Security Data System.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has completed fraud assessments for three types of immigration benefits—having completed two at the time of our March 2006 report—and expects to issue final reports on four additional assessments later in fiscal year 2007. However, USCIS has not yet fully developed a comprehensive strategy for conducting benefit fraud assessments. Until DHS does so and demonstrates successful application of a strategy and approach for conducting fraud assessment, we conclude that DHS has generally not achieved this performance expectation. In addition, DHS has taken actions to develop a data system to identify fraud through automated analysis tools. However, this data analysis capability has not yet been fully implemented. |  |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

## DHS Has Made Moderate Progress in Securing the Aviation Sector

DHS has implemented a variety of programs to help secure the aviation sector. Within the department, TSA is the primary agency with responsibility for aviation security efforts. TSA was established in 2001 with the mission to protect the transportation network while also ensuring the free movement of people and commerce. Since its inception, TSA has focused much of its efforts on aviation security and has developed and implemented a variety of programs and procedures to secure commercial aviation. For example, TSA has undertaken efforts to strengthen airport security; provide and train a screening workforce; prescreen passengers against terrorist watch lists; and screen passengers, baggage, and cargo. TSA has implemented these efforts in part to meet numerous mandates for strengthening aviation security placed on the agency following the September 11, 2001, terrorist attacks. These mandates set priorities for the agency and guided TSA's initial efforts to enhance aviation security. In addition to TSA, CBP, and DHS's Science and Technology Directorate play roles in securing commercial aviation. In particular, CBP has responsibility for conducting passenger prescreening—or the matching of passenger information against terrorist watch lists—for international flights operating to or from the United States, as well as inspecting inbound air cargo upon its arrival in the United States. The Science and Technology Directorate is responsible for the research and development of aviation security technologies.

As shown in table 22, we identified 24 performance expectations for DHS in the area of aviation security, and we found that overall DHS has made moderate progress in meeting those expectations. Specifically, we found that DHS has generally achieved 17 performance expectations and has generally not achieved 7 performance expectations.

**Table 22: Performance Expectations and Progress Made in Aviation Security**

| | Assessment | | |
|---|---|---|---|
| **Performance expectation** | **Generally achieved** | **Generally not achieved** | **No assessment made** |
| 1. Implement a strategic approach for aviation security functions | ✓ | | |
| 2. Establish standards and procedures for effective airport perimeter security | | ✓ | |
| 3. Establish standards and procedures to effectively control access to airport secured areas | | ✓ | |
| 4. Establish procedures for implementing biometric identifier systems for airport secured areas access control | | ✓ | |
| 5. Ensure the screening of airport employees against terrorist watch lists | ✓ | | |
| 6. Hire and deploy a federal screening workforce | ✓ | | |
| 7. Develop standards for determining aviation security staffing at airports | ✓ | | |
| 8. Establish standards for training and testing the performance of airport screener staff | ✓ | | |
| 9. Establish a program and requirements to allow eligible airports to use a private screening workforce | ✓ | | |
| 10. Train and deploy federal air marshals on high-risk flights | ✓ | | |
| 11. Establish standards for training flight and cabin crews | ✓ | | |

| | Assessment | | |
|---|---|---|---|
| Performance expectation | Generally achieved | Generally not achieved | No assessment made |
| 12. Establish a program to allow authorized flight deck officers to use firearms to defend against any terrorist or criminal acts | ✓ | | |
| 13. Establish policies and procedures to ensure that individuals known to pose, or suspected of posing, a risk or threat to security are identified and subjected to appropriate action | ✓ | | |
| 14. Develop and implement an advanced prescreening system to allow DHS to compare domestic passenger information to the Selectee List and No Fly List | | ✓ | |
| 15. Develop and implement an international passenger prescreening process to compare passenger information to terrorist watch lists before aircraft departure | | ✓ | |
| 16. Develop and implement processes and procedures for physically screening passengers at airport checkpoints | ✓ | | |
| 17. Develop and test checkpoint technologies to address vulnerabilities | ✓ | | |
| 18. Deploy checkpoint technologies to address vulnerabilities | | ✓ | |
| 19. Deploy explosive detection systems (EDS) and explosive trace detection (ETD) systems to screen checked baggage for explosives | ✓ | | |
| 20. Develop a plan to deploy in-line baggage screening equipment at airports | ✓ | | |
| 21. Pursue the deployment and use of in-line baggage screening equipment at airports | ✓ | | |
| 22. Develop a plan for air cargo security | ✓ | | |
| 23. Develop and implement procedures to screen air cargo | ✓ | | |
| 24. Develop and implement technologies to screen air cargo | | ✓ | |
| **Total** | **17** | **7** | **0** |

Source: GAO analysis.

Note: An assessment of “generally achieved” indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of “generally achieved” does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, “generally not achieved” indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of “generally not achieved” may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated “no assessment made.”

Table 23 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of aviation security and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation's key elements (generally not achieved).

Table 23: Performance Expectations and Assessment of DHS Progress in Aviation Security

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Implement a strategic approach for aviation security functions | *GAO findings:* DHS has adhered to a strategic approach for implementing its aviation security functions, governed largely by legislative requirements. TSA, which has responsibility for securing all modes of transportation, has also taken steps to ensure that it implements its aviation security functions in a strategic manner. For example, in April 2006, we reported that TSA has spent billions of dollars and implemented a wide range of initiatives to strengthen the key components of its passenger and checked baggage screening systems—people, processes, and technology. These components are interconnected and are critical to the overall security of commercial aviation. For more information, see *Aviation Security: Enhancements Made in Passenger and Checked Baggage Screening, but Challenges Remain*, GAO-06-371T.<br>*DHS updated information:* In March 2007, the National Strategy on Aviation Security and its six supporting plans were released. The six supporting plans are Aviation Transportation System Security, Aviation Operational Threat Response, Aviation Transportation System Recovery, Aviation Domain Surveillance and Intelligence Integration, Domestic Outreach, and International Outreach. According to TSA, an Interagency Implementation Working Group was established under TSA leadership in January 2007 to initiate implementation efforts for the 112 actions specified in the supporting plans.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation, as DHS has taken a strategic approach to implementing its aviation security functions, and the National Strategy on Aviation Security has been issued. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 2. Establish standards and procedures for effective airport perimeter security | *GAO findings:* In June 2004, we reported on TSA's efforts to strengthen the security of airport perimeters (such as airfield fencing and access gates), the adequacy of controls restricting unauthorized access to secured areas (such as building entryways leading to aircraft), and security measures pertaining to individuals who work at airports. At the time of our review, we found TSA had begun evaluating commercial airport security but had not yet implemented a number of congressionally mandated requirements. We reported that TSA had begun evaluating the security of airport perimeters, but had not yet determined how the results of these evaluations could be used to make improvements to the nation's airport system as a whole. Specifically, we found that TSA had begun conducting regulatory compliance inspections, covert testing of selected security procedures, and vulnerability assessments at selected airports. These evaluations, though not yet complete at the time of our report, identified perimeter security concerns. In addition, we reported that TSA intended to compile baseline data on security vulnerabilities to enable it to conduct a systematic analysis of airport security vulnerabilities on a nationwide basis. TSA said such an analysis was essential since it would allow the agency to determine minimum standards and the adequacy of security policies and help the agency and airports better direct limited resources. Nonetheless, at the time of our review, TSA had not yet developed a plan that prioritized its assessment efforts, provided a schedule for completing these assessments, or described how assessment results would be used to help guide agency decisions on what, if any, security improvements were needed. We are conducting follow-on work in this area. For more information, see *Aviation Security: Transportation Security Administration Has Made Progress in Managing a Federal Security Workforce and Ensuring Security at U.S. Airports, but Challenges Remain,* GAO-06-597T and *Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls,* GAO-04-728.<br>*DHS updated information:* In April and July 2007, DHS provided us with updated sensitive information on efforts to secure airport perimeters. This information described TSA's plans to assess technology being used to enhance perimeter security, as well as a summary of TSA's policies and procedures related to perimeter security. DHS also provided us with updated sensitive information on its efforts to enhance security procedures for gate screening, aircraft cabin searches, and security measures for personnel identification media.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. While DHS has taken actions to enhance perimeter security, DHS did not provide us with evidence that these actions provide for effective airport perimeter security and thus satisfy the intent of this performance expectation. DHS also did not provide information or documentation that it had addressed all of the relevant requirements established in the Aviation and Transportation Security Act and our 2004 recommendations related to (1) identifying security weaknesses of the commercial airport system as a whole, (2) prioritizing funding to address the most critical needs, or (3) reducing the risks posed by airport workers. Until DHS demonstrates how the security efforts it has undertaken have strengthened commercial airport perimeters security, it will be difficult for it to justify its resources needs and clearly identify progress made in the area. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 3. Establish standards and procedures to effectively control access to airport secured areas | *GAO findings and DHS IG findings:* In June 2004 we reported that TSA had begun evaluating the controls that limit access into secured airport areas, but had not completed actions to ensure that all airport workers employed in these areas were vetted prior to being hired and trained. We also reported that TSA had begun evaluating the security of the controls that limited access into secured airport areas, but had not yet determined how the results of these evaluations could be used to make improvements to the nation's airport system as a whole. Specifically, we found that TSA had begun conducting regulatory compliance inspections, covert testing of selected security procedures, and vulnerability assessments at selected airports. These evaluations—though not completed at the time of our report—identified access control security concerns. For example, TSA identified instances where airport operators failed to comply with existing security requirements. In addition, we reported that TSA intended to compile baseline data on security vulnerabilities to enable it to conduct a systematic analysis of airport security vulnerabilities on a nationwide basis. TSA said such an analysis was essential since it would allow the agency to determine minimum standards and the adequacy of security policies and help the agency and airports better direct limited resources. Nonetheless, at the time of our review, TSA had not yet developed a plan that prioritized its assessment efforts, provided a schedule for completing these assessments, or described how assessment results would be used to help guide agency decisions on what, if any, security improvements were needed. More recently, in March 2007, the DHS IG reported the results of its access control testing at 14 domestic airports of various sizes nationwide. As a result of more than 600 access control tests, the DHS IG identified various recommendations to enhance the overall effectiveness of controls that limit access to airport secured areas. We are conducting follow-on work in this area. For more information, see GAO-06-597T and GAO-04-728. See also Department of Homeland Security Office of Inspector General, *Audit of Access to Airport Secured Areas* (Unclassified Summary), OIG-07-35 (Washington, D.C., March 15, 2007).<br>*DHS updated information:* In March, April, and July 2007, DHS provided us with updated information on its efforts to establish standards and procedures for effective access control of airport secured areas. TSA reported that its Aviation Direct Access Screening Program was piloted in March 2006 and disseminated to Federal Security Directors in August 2006 to provide for random screening of airport and airline employees and employees' property and vehicles as they enter secure areas of airports. Transportation security officers screen for the presence of explosives, incendiaries, weapons, and other items of interest as well as improper airport identification. TSA reported that the Aviation Direct Access Screening Program was reissued in March 2007 to include boarding gate screening and aircraft cabin searches and to mandate participation for airports nationwide. TSA also reported that it verifies the identification of individuals present in airport secured areas and assists operators and air carriers in performance of security responsibilities. DHS also provided us with updated sensitive information on its efforts to enhance security procedures for gate screening, aircraft cabin searches, and security measures for personnel identification media, as well as a description of TSA's plans to assess technology being used to enhance access controls and a summary of TSA's access control policies and procedures.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has taken actions to establish procedures for access control of airport secured areas. However, DHS did not provide us with evidence that these actions provide for effective access control for airport secured areas and thus satisfy the intent of this performance expectation. Additionally, DHS did not provide information or documentation that it had addressed all of the relevant requirements established in the Aviation and Transportation Security Act and our 2004 recommendations related to (1) identifying security weaknesses of the commercial airport system as a whole, (2) prioritizing funding to address the most critical needs, or (3) reducing the risks posed by airport workers. The recent assessment by the DHS OIG identified continuing weaknesses in TSA's procedures to prevent unauthorized individuals from access to secured airport areas. Until DHS demonstrates how the security efforts it has undertaken have strengthened the security of airport access controls, it will be difficult for it to justify its resource needs and clearly identify progress in this area. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 4. Establish procedures for implementing biometric identifier systems for airport secured areas access control | *GAO findings:* In June 2004, we reported that TSA had begun efforts to evaluate the effectiveness of security-related technologies, such as biometric identification systems. However, we reported that TSA had not developed a plan for implementing new technologies or balancing the costs and effectiveness of these technologies with the security needs of individual airports and the commercial airport system as a whole. In September 2005, TSA issued a guidance package for biometrics for airport access control. This guidance was primarily directed at airport operators who own and operate access control systems at airports and manufacturers of biometric devices who would need to submit their devices for qualification, including performance testing, in order to be potentially placed on a TSA biometric Qualified Products List. The guidance package includes information on technical and operational requirements and standards, implementation guidance, and a plan for biometric qualified products list.<br>*DHS updated information:* DHS did not provide us with updated information on its efforts to establish procedures for implementing biometric identifier systems.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although TSA issued a guidance package, we reported in April 2007 that DHS and industry stakeholders continue to face difficult challenges in ensuring that the biometric access control technologies will work effectively in the maritime environment where the Transportation Worker Identification Credential program (DHS's effort to develop biometric access control systems to verify the identity of individuals accessing secure transportation areas) is being initially tested. Because of the challenges in implementing the system in the maritime environment, DHS has not yet determined how and when it will implement a biometric identification system for access controls at commercials airports. We have initiated ongoing work to further assess DHS's efforts to establish procedures for implementing biometric identifier systems for airport secured areas access control. | Generally not achieved |
| 5. Ensure the screening of airport employees against terrorist watch lists | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation, as it has worked to ensure the screening of airport employees against terrorist watch lists. We reported that TSA requires most airport workers who perform duties in secured and sterile areas to undergo a fingerprint-based criminal history records check. TSA further requires airport operators to compare applicants' names against the No Fly List and Selectee List. Once workers undergo this review, they are granted access to airport areas in which they perform duties. For more information, see GAO-06-597T and GAO-04-728. | Generally achieved |
| 6. Hire and deploy a federal screening workforce | *GAO findings:* DHS has hired and deployed a federal screening workforce at airports. TSA initially deployed over 50,000 screeners (now called transportation security officers) at over 440 commercial airports nationwide. However, TSA has experienced staffing shortages, and we reported that to accomplish its security mission, TSA needs a sufficient number of passenger and checked baggage transportation security officers trained and certified in the latest screening procedures and technology. We reported in February 2004 that staffing shortages and TSA's hiring process had hindered the ability of some Federal Security Directors to provide sufficient resources to staff screening checkpoints and oversee screening operations at their checkpoints without using additional measures such as overtime. TSA has taken action to address some of these staffing challenges by, for example, developing a model to determine the most appropriate allocation of transportation security officers among airports and implementing human capital initiatives to address hiring and retention challenges. For more information, see GAO-06-597T; *Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining*, GAO-03-1173; and *Aviation Security: TSA's Staffing Allocation Model Is Useful for Allocating Staff among Airports, but Its Assumptions Should Be Systematically Reassessed*, GAO-07-299.<br>*DHS updated information:* In March 2007, DHS reported that TSA deployed a pay-for-performance system, called Performance Accountability and Standards System, for transportation security officers, lead and supervisory transportation security officers, and screening managers. TSA also reported that it has developed a local, decentralized hiring process to give Federal Security Directors more control over aspects of hiring. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | *Our assessment:* We conclude that DHS has generally achieved this performance expectation. We have not yet fully evaluated TSA's pay-for-performance system or its hiring process. However, DHS has hired and deployed a federal screening workforce at airports. | |
| 7. Develop standards for determining aviation security staffing at airports | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation as DHS has developed standards for determining aviation security staffing levels. In June 2005, TSA submitted its report on aviation security staffing standards to Congress. Known as the Staffing Allocation Model, these standards are intended to provide an objective measure for determining staffing levels for transportation security officers, while staying within the congressionally mandated limit of 45,000 full-time equivalent screeners. In February 2007, we reported that TSA's Staffing Allocation Model is intended to provide a sufficient number of transportation security officers—or screeners—to perform passenger and checked baggage screening through built-in assumptions, which are designed to ensure the necessary levels of security and to minimize wait times, along with multiple monitoring mechanisms to assess the sufficiency of the model's outputs. However, we identified concerns with some of the fiscal year 2006-model assumptions. Further, although TSA officials stated that they plan to conduct an annual review of select assumptions, and based changes to the fiscal year 2007 model on such a review, TSA does not have a mechanism in place for prioritizing its review and for ensuring that all assumptions are periodically validated to help ensure that they reflect operating conditions. We reported that TSA risks basing its staffing allocations on assumptions that do not reflect operating conditions if periodic validations are not conducted. For more information, see GAO-06-597T; *Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains,* GAO-07-448T; and GAO-07-299. | Generally achieved |
| 8. Establish standards for training and testing the performance of airport screener staff | *GAO findings:* DHS has established standards for training and testing airport transportation security officers. For example, TSA introduced an Online Learning Center that made self-guided courses available over the Internet. In December 2005, TSA reported completing enhanced explosives detection training for over 18,000 transportation security officers. TSA also implemented and strengthened efforts to collect performance data on the effectiveness of screening operations. For example, TSA increased its use of covert testing to assess the performance of screening operations. However, we identified concerns with transportation security officers' access to online training. In May 2005, we also noted that TSA had not yet begun to use data from local covert testing to identify training and performance needs because of difficulties in ensuring that local covert testing was implemented consistently nationwide, although TSA is taking some actions to address this issue. In April 2007, we reported that TSA monitors transportation security officers' compliance with passenger checkpoint screening standard operating procedures through its performance accountability and standards system and through local and national covert testing. According to TSA officials, the agency developed the performance accountability and standards system in response to our 2003 report that recommended that TSA establish a performance management system that makes meaningful distinctions in employee performance and in response to input from TSA airport staff on how to improve passenger and checked baggage screening measures. This system is used by TSA to measure transportation security officers' compliance with passenger checkpoint screening procedures. We have ongoing work assessing TSA's covert testing program, which we will complete later this year. For more information, see GAO-597T; *Aviation Security: Screener Training and Performance Measurement Strengthened, but More Work Remains,* GAO-05-457; and GAO-07-448T.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to train and test the performance of airport screener staff. TSA reported that its Aviation Screening Assessment Program, which is to be implemented at all airports this year, is intended to use local screening workforce and Bomb Appraisal Officers to perform covert testing of passenger and baggage screening capabilities. TSA reported that the program is intended to measure screening performance using standardized test scenarios. In addition, TSA reported that it is implementing Improvised Explosive Devices Checkpoint Screening Drills in which transportation security officers | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | will be routinely exposed to simulated items, without warning.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation, as DHS has established standards for training and testing for airport transportation security officers. | |
| 9. Establish a program and requirements to allow eligible airports to use a private screening workforce | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation, as DHS has taken actions to establish a program that allows eligible airports to use private screeners. In March 2006, we reported that TSA created the Screening Partnership Program to allow all commercial airports an opportunity to apply to TSA for permission to use qualified private screening contractors and private sector screeners. We noted that TSA developed performance goals and began drafting related measures and targets to assess the performance of private screening contractors under the Screening Partnership Program in the areas of security, customer service, costs, workforce management, and innovation. However, we noted that as TSA moved forward with this program, it had opportunities to strengthen the management and oversight of the program, including providing clear guidance to program applicants on their roles and responsibilities at airports where a privatized screener workforce operates and identifying the underlying reasons for the small number of program applicants. For more information, see *Aviation Security: Progress Made to Set Up Program Using Private-Sector Airport Screeners, but More Work Remains,* GAO-06-166 and *Aviation Security: Preliminary Observations on TSA's Progress to Allow Airports to Use Private Passenger and Baggage Screening Services,* GAO-05-126. | Generally achieved |
| 10. Train and deploy federal air marshals on high-risk flights | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation, as DHS has trained and deployed federal air marshals on flights deemed high-risk. To carry out its mission, the Federal Air Marshal Service deploys federal air marshals on board flights either destined for or originating in the United States. Deployed to passenger flights, federal air marshals dress in plain clothes to blend in with other passengers and perform their duties discreetly in an effort to avoid drawing undue attention to themselves. We have ongoing work assessing the Federal Air Marshal Service program. For more information, see *Aviation Security: Federal Air Marshal Service Could Benefit from Improved Planning and Controls,* GAO-06-203. | Generally achieved |
| 11. Establish standards for training flight and cabin crews | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation, as it has established standards for training flight and cabin crews. In September 2005, we reported that TSA enhanced guidance and standards for flight and cabin crew member security training with input from stakeholders. Specifically, TSA revised the guidance and standards to include additional training elements required by law and to improve the organization and clarity of the guidance and standards. TSA also took steps to strengthen its efforts to oversee air carriers' flight and cabin crew security training to ensure they were complying with the required guidance and standards. For example, in January 2005, TSA added staff with expertise in designing training programs to review air carriers' crew member security training curriculums and developed a standard form for staff to use to conduct their reviews. TSA also developed an advanced voluntary self-defense training program with input from stakeholders and implemented the program in December 2004. However, we noted that TSA had not established strategic goals and performance measures for assessing the effectiveness of the training because it considered its role in the training program as regulatory. We also noted that TSA lacked adequate controls for monitoring and reviewing air carriers' crew member security training, including written procedures for conducting and documenting these reviews. For more information, see *Aviation Security: Flight and Cabin Crew Member Security Training Strengthened, but Better Planning and Internal Controls Needed,* GAO-05-781. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 12. Establish a program to allow authorized flight deck officers to use firearms to defend against any terrorist or criminal acts | *GAO and DHS IG findings:* According to the DHS IG, TSA's Federal Flight Deck Officer program is to select, train, deputize, arm with handguns, and supervise volunteer airline pilots and other flight deck crew members for the purpose of defending the flight decks of passenger and cargo aircraft. The IG reported in December 2006, they surveyed a sample of federal flight deck officers to identify pilot concerns about the Federal Flight Deck Officer program. Pilot concerns included not being given time off to attend training, the remote location of the training and the amount of time needed to get to the training site, TSA's weapons carriage policy, and the type of credentials used to identify federal flight deck officers. These concerns may have dissuaded pilots from participating in the program, thus reducing the number of federal flight deck officers. In December 2005, management of the Federal Flight Deck Officer program was assigned to TSA's Office of Law Enforcement-Federal Air Marshal Service. This office established focus groups to foster communications among the federal flight deck officer community, the airline industry, and professional associations, and to address federal flight deck officer operational concerns. Also, the office management established a federal flight deck officer working group to assess recommendations on proposals concerning federal flight deck officer credentials and badges, checkpoint requirements, weapons issues (including transport, storage, and qualifications), communications protocols, training, and industry liaison. While TSA has now trained and deputized federal flight deck officers and has addressed various procedural and process issues, the DHS IG concluded that more needed to be accomplished to maximize the use of federal flight deck officers on international and domestic flights. TSA continues to work with federal flight deck officers, Federal Security Directors, and industry to improve Federal Flight Deck Officer program effectiveness. For more information, see Department of Homeland Security Office of Inspector General, *Improvements Needed in TSA's Federal Flight Deck Officer Program,* OIG-07-14 (Washington, D.C.: December 2006).<br>*DHS updated information:* In March 2007, DHS reported that it has implemented a Federal Flight Deck Officer program for all-cargo aircraft operators and noted that this program provides training to pilots, program management, resources, and equipment to protect the aircraft.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. The DHS IG reported that TSA has established and is working to improve the Federal Flight Deck Officer Program. However, the DHS IG also reported that a variety of challenges have affected the program, including the amount of time and location of training, the weapons carriage policy, and type of credentials used to identify federal flight deck officers. | Generally achieved |
| 13. Establish policies and procedures to ensure that individuals known to pose, or suspected of posing, a risk or threat to security are identified and subjected to appropriate action | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. TSA ensures that all passengers on domestic flights are checked against the Selectee List and No Fly List. Passenger prescreening is used to identify passengers who may pose a higher risk to aviation security than other passengers and therefore should receive additional and more thorough security scrutiny. Air carriers check passenger information against government supplied watch lists that contain the names of individuals who, for certain reasons, are either not allowed to fly (the No Fly List) or pose a higher than normal risk and therefore require additional security attention (the Selectee List). Passengers on the No Fly List are denied boarding passes and are not permitted to fly unless cleared by law enforcement officers. Passengers who are on the Selectee List are issued boarding passes, and they and their baggage undergo additional security measures. For more information, see *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed,* GAO-05-356. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 14. Develop and implement an advanced prescreening system to allow DHS to compare domestic passenger information to the Selectee List and No Fly List | *GAO findings:* DHS is developing an advanced passenger prescreening system called Secure Flight. However, TSA has faced challenges in developing and implementing Secure Flight and has not yet completed its development efforts. In 2006 we reported that TSA had not conducted critical activities in accordance with best practices for large-scale information technology programs and had not followed a disciplined life cycle approach in developing Secure Flight, in which all phases of the project are defined by a series of orderly steps and the development of related documentation. We also found that while TSA had taken steps to implement an information security management program for protecting Secure Flight information and assets, its efforts were incomplete, based on federal standards and industry best practices. In addition, in 2006 we reported that prior to TSA's rebaselining effort of Secure Flight, several oversight reviews of the program had been conducted that raised questions about program management, including the lack of fully defined requirements. In January 2007, TSA reported that it has completed its rebaselining efforts, which included reassessing program goals and capabilities and developing a new schedule and cost estimates. However, we have not yet assessed TSA's progress in addressing past problems. In February 2007, we reported that as TSA moves forward with Secure Flight, it will need to employ a range of program management disciplines, which we previously found missing, to control program cost, schedule, performance, and privacy risks. We have ongoing work reviewing DHS's efforts to develop and implement Secure Flight, including progress made during its rebaselining efforts. For more information, see *Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program,* GAO-06-864T; *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notes, but Has Recently Taken Steps to More Fully Inform the Public,* GAO-05-864R; and *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed,* GAO-05-356.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to develop and implement Secure Flight. DHS reported that as a result of its rebaselining efforts, government controls were developed to implement Secure Flight, and DHS provided information on Secure Flight's technical and system engineering management plans and requirements, concept of operations, risk assessments, and privacy issues. DHS reported that it plans to begin parallel operations with the first groups of domestic aircraft operators in the first quarter of fiscal year 2009 and to take over full responsibility for watch list matching in fiscal year 2010.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS is continuing efforts to develop the Secure Flight program, but has not yet completed its development efforts and has not yet implemented the program. | Generally not achieved |
| 15. Develop and implement an international passenger prescreening process to compare passenger information to terrorist watch lists before aircraft departure | *GAO findings:* DHS has not yet implemented enhancements to its passenger prescreening process for passengers on international flights departing from or bound to the United States. We recently reported that the existing identity-matching component of DHS's process involves separate matching activities conducted by air carriers (prior to a flight's departure and pursuant to TSA requirements) and by CBP (generally after a flight's departure). We reported that as with domestic passenger prescreening, air carriers conduct an initial match of self-reported passenger name record data against the No Fly List and Selectee List before international flight departures. CBP's process, in effect, supplements the air carrier identity-matching for international flights by comparing additional passenger information collected from passports (this information becomes part of Advanced Passenger Information System data), against the No Fly List and Selectee List and other government databases. Under current federal regulations for CBP's prescreening of passengers on international flights, air carriers are required to provide the U.S. government with passenger name record data as well as Advanced Passenger Information System data to allow the government to conduct, among other things, identity matching procedures against the No Fly List and Selectee List—which typically occur just after or at times just before the departure of international flights traveling to or from the United States, respectively. To address a concern that the federal government's identity matching may not be conducted in a timely manner, in 2004, | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | Congress mandated that DHS issue a proposed rule requiring that the U.S. government's identity-matching process occur before the departure of international flights. CBP published this proposed rule in July 2006 and, if implemented, it would allow the U.S. government to conduct passenger prescreening in advance of flight departure, and would eliminate the need for air carriers to continue performing an identity-matching function for international flights. For more information, see GAO-07-448T and *Aviation Security: Efforts to Strengthen International Passenger Prescreening Are Under Way, but Planning and Implementation Issues Remain,* GAO-07-346.<br>*DHS updated information:* In March 2007, TSA reported that it was working with CBP to combine the predeparture Advance Passenger Information System and Secure Flight into one DHS solution.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. We identified various problems with DHS's implementation of the international prescreening process and made recommendations to help address some of those concerns. In addition, while efforts to define functional requirements and operations are underway for aligning international and domestic passenger prescreening, full implementation of an integrated system will not occur for several years, as Secure Flight is not yet operational for domestic passenger prescreening. | |
| 16. Develop and implement processes and procedures for physically screening passengers at airport checkpoints | *GAO findings:* DHS has developed and implemented processes and procedures for screening passengers at checkpoints. Passenger screening is a process by which authorized TSA personnel inspect individuals and property to deter and prevent the carriage of any unauthorized explosives, incendiary, weapon, or other dangerous item onboard an aircraft or into a sterile area. Authorized TSA personnel must inspect individuals for prohibited items at designated screening locations. The passenger-screening functions are X-ray screening of property, walk-through metal detector screening of individuals, hand-wand or pat-down screening of individuals, physical search of property and trace detection for explosives, and behavioral observation. We have also reported that TSA has developed processes and procedures for screening passengers at security checkpoints, balancing security needs with efficiency and customer service considerations. TSA has also revised these policies and procedures to generally improve the efficiency, effectiveness, and clarity of the procedures, but could improve the evaluation of procedures before they are implemented. In April 2007, we reported that standard operating procedures modifications were proposed based on the professional judgment of TSA senior-level officials and program-level staff. In some cases, TSA tested proposed modifications at selected airports to help determine whether the changes would achieve their intended purpose. However, we reported that TSA's data collection and analyses could be improved to help TSA determine whether proposed procedures that are operationally tested would achieve their intended purpose. We also reported that TSA's documentation on proposed modifications to screening procedures was not complete. We noted that without more complete documentation, TSA may not be able to justify key modifications to passenger screening procedures to Congress and the traveling public. For more information, see *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved,* GAO-07-634; *Aviation Security: TSA's Change to Its Prohibited Items List Has Not Resulted in Any Reported Security Incidents, but the Impact of the Change on Screening Operations Is Inconclusive,* GAO-07-623R; GAO-03-1173; and GAO-06-371T.<br>*DHS updated information:* In March 2007, DHS reported that it trained tens of thousands of transportation security officers and took various regulatory actions to address concerns regarding liquids and gels carried aboard aircraft. DHS reported that TSA worked with technical experts and counterparts in other countries to harmonize security procedures. TSA also reported making changes to the Prohibited Items List to allow transportation security officers to focus on detecting high-risk threats which have the ability to cause catastrophic damage, such as improvised explosive devices. Moreover, TSA provided information on two recent initiatives intended to strengthen the passenger checkpoint screening process. TSA's Screening Passenger by Observation Technique program is a behavior observation and analysis program designed to provide TSA Behavior Detection Officers with a nonintrusive means of identifying potentially high- | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | risk individuals who exhibit behaviors indicative of inordinate levels of stress, fear, and/or deception that could indicate possible terrorist or criminal activity. TSA reported that this program is implemented using a threat-based strategy and is based on other behavioral analysis programs used by law enforcement and security personnel. In addition, TSA's Travel Document Checker program replaces current travel document checkers with transportation security officers who have access to sensitive security information on the threat posture of the aviation industry and check for fraudulent documents.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation, as DHS has developed and implemented processes and procedures for screening passengers at airport checkpoints. | |
| 17. Develop and test checkpoint technologies to address vulnerabilities | *GAO findings:* DHS has undertaken efforts to develop and test checkpoint technologies to address vulnerabilities that may be exploited by identified threats such as improvised explosive devices. For example, TSA recently placed increased focus on the threats posed by liquid explosives and has been developing technology to automatically detect liquid explosives in bottles. TSA has also been modifying commercial-off-the-shelf technologies to mitigate threats posed by passengers bearing improvised explosive devices. However, these machines do not automatically detect explosives. For example, TSA is modifying a whole body image to screen passengers for explosives, plastics, and metals otherwise obfuscated by clothing. The machine uses x-ray backscatter technology to produce an image that transportation security officers interpret. We are currently reviewing DHS and TSA's efforts to develop and test technologies and will be reporting on these efforts later this year. For more information, see GAO-06-371T.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to develop and test checkpoint technologies. TSA reported that it is exploring portable explosive detection system units and explosive trace portals at various airport locations and is operationally testing a whole body imaging system. TSA also reported that it is planning to pilot test a cast and prosthetics screening technology and an automated explosives detection system for carry-on baggage. TSA also reported that, in partnership with the Science and Technology Directorate, it is assessing the capabilities of advanced x-ray technologies to provide enhanced capabilities in the detection of improvised explosives devices in carry-on items.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has reported taking actions to develop and test checkpoint technologies. The full extent of DHS's efforts is the focus of an ongoing GAO review scheduled for completion later this year. | Generally achieved |
| 18. Deploy checkpoint technologies to address vulnerabilities | *GAO findings:* DHS has not yet deployed checkpoint technologies to address key existing vulnerabilities. For example, in July 2006, TSA provided us with information that 97 explosives trace portal machines had been installed at over 37 airports. This new technology uses puffs of air to help detect the presence of explosives on individuals. However, DHS identified problems with these machines and has halted their deployment. DHS's fiscal year 2007 budget request stated that TSA expected that 434 explosives trace portal machines would be in operation throughout the country by September 2007. TSA is also developing backscatter technology, but limited progress has been made in fielding this technology at airport passenger screening checkpoints. We are currently reviewing TSA's technology development and deployment efforts and will be reporting on these efforts later this year. For more information, see GAO-06-371T.<br>*DHS updated information:* DHS reported in March 2007 that extensive deployment of new technologies will not be realized for another 2 years.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has faced challenges and delays in deploying checkpoint technologies to effectively address vulnerabilities, and TSA has reported that deployment of new technologies is likely 2 years away. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 19. Deploy EDS and ETD systems to screen checked baggage for explosives | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation, as TSA has deployed EDS and ETD systems at the nation's airports. From November 2001 through June 2006, TSA procured and installed about 1,600 EDS machines and about 7,200 ETD machines to screen checked baggage for explosives at over 400 commercial airports. TSA made progress in fielding EDS and ETD equipment at the nation's airports, placing this equipment in a stand-alone mode—usually in airport lobbies—to conduct the primary screening of checked baggage for explosives, due to congressional mandates to field the equipment quickly and limitations in airport design. For more information, see *Aviation Security: TSA Oversight of Checked Baggage Screening Procedures Could Be Strengthened,* GAO-06-869 and GAO-06-371T. | Generally achieved |
| 20. Develop a plan to deploy in-line baggage screening equipment at airports | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed a plan to deploy in-line baggage screening equipment at airports, based in part on a recommendation we made. The plan is aimed at increasing security through deploying more EDS machines, lowering program life-cycle costs, minimizing impacts on TSA and airport and airline operations, and providing a flexible security infrastructure. In March 2005, we reported that at nine airports where TSA had agreed to help fund the installation of in-line EDS systems, TSA estimated that screening with in-line EDS machines could save the federal government about $1.3 billion over 7 years. In February 2006, TSA reported that many of the initial in-line EDS systems did not achieve the anticipated savings. However, recent improvements in the design of the in-line EDS systems and EDS screening technology offer the opportunity for higher-performance and lower-cost screening systems. Screening with in-line EDS systems may also result in security benefits by reducing the need for TSA to use alternative screening procedures, such as screening with explosives detection canines and physical bag searches, which involve trade-offs in security effectiveness. For more information, see GAO-06-869; GAO-06-371T; and GAO-07-448T. | Generally achieved |
| 21. Pursue the deployment and use of in-line baggage screening equipment at airports | *GAO findings:* Despite delays in the widespread deployment of in-line systems due to the high upfront capital investment required, DHS is pursuing the deployment and use of in-line explosives detection equipment and is seeking creative financing solutions to fund the deployment of these systems. TSA determined that recent improvements in the design of the in-line EDS systems and EDS screening technology offer the opportunity for higher performance and lower cost screening systems. Screening with in-line EDS systems could also result in security benefits by reducing congestion in airport lobbies and reducing the need for TSA to use alternative screening procedures, such as screening with explosives detection canines and physical bag searches. TSA's use of these procedures, which are to be used only when volumes of baggage awaiting screening pose security vulnerabilities or when TSA officials determine that there is a security risk associated with large concentrations of passengers in an area, has involved trade-offs in security effectiveness. TSA has begun to systematically plan for the optimal deployment of checked baggage screening systems, but resources have not been made available by Congress to fund the installation of in-line EDS machines on a large-scale basis. TSA reported that as of June 2006, 25 airports had operational in-line EDS systems and an additional 24 airports had in-line systems under development. In May 2006, TSA reported that under current investment levels, installation of optimal checked baggage screening systems would not be completed until approximately 2024. For more information, see GAO-06-869 and GAO-06-371T.<br>*DHS updated information:* In March 2007, DHS reported that it is working with its airport and air carrier stakeholders to improve checked baggage screening solutions and to look creatively at in-line baggage screening system solutions to enhance security and free up lobby space at airports.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has undertaken efforts to deploy and use in-line baggage screening equipment, but challenges exist to deploying in-line systems due to the high costs of the systems and questions regarding how the systems will be funded. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 22. Develop a plan for air cargo security | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed a strategic plan for domestic air cargo security and has taken actions to use risk management principles to guide investment decisions related to air cargo bound for the United States from a foreign country, referred to as inbound air cargo, but these actions are not yet complete. With regard to domestic air cargo, we reported that TSA completed an Air Cargo Strategic Plan in November 2003 that outlined a threat-based risk management approach to securing the nation's air cargo transportation system. TSA's plan identified strategic objectives and priority actions for enhancing air cargo security based on risk, cost, and deadlines. With regard to inbound air cargo, in April 2007, we reported that TSA and CBP have taken some preliminary steps to use risk management principles to guide their investment decisions related to inbound air cargo, as advocated by DHS, but most of these efforts are in the planning stages. We reported that although TSA completed a risk-based strategic plan to address domestic air cargo security, it has not developed a similar strategy for addressing inbound air cargo security, including how best to partner with CBP and international air cargo stakeholders. Further, TSA has identified the primary threats associated with inbound air cargo, but has not yet assessed which areas of inbound air cargo are most vulnerable to attack and which inbound air cargo assets are deemed most critical to protect. TSA plans to assess inbound air cargo vulnerabilities and critical assets—two crucial elements of a risk-based management approach—but has not yet established a methodology or time frame for how and when these assessments will be completed. Without such assessments, we reported that TSA may not be able to appropriately focus its resources on the most critical security needs. We recommended that TSA more fully develop a risk-based strategy to address inbound air cargo security, including establishing goals and objectives for securing inbound air cargo and establishing a methodology and time frames for completing assessments of inbound air cargo vulnerabilities and critical assets that can be used to help prioritize the actions necessary to enhance security. For more information, see *Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security,* GAO-06-76, and *Aviation Security: Federal Efforts to Secure U.S.-Bound Air Cargo Are in the Early Stages and Could Be Strengthened,* GAO-07-660. | Generally achieved |
| 23. Develop and implement procedures to screen air cargo | *GAO findings:* DHS has taken actions to develop and implement procedures for screening domestic air cargo.[a] With regard to domestic air cargo, air carriers are responsible for implementing TSA security requirements that include measures related to the acceptance, handling, and inspection of cargo; training of employees in security and cargo inspection procedures; testing employee proficiency in cargo inspection; and access to cargo areas and aircraft, and TSA inspects carriers' compliance. We reported in October 2005 that TSA had significantly increased the number of domestic air cargo inspections conducted of air carrier and indirect air carrier compliance with security requirements. We also reported that TSA exempted certain cargo from random inspection because it did not view the exempted cargo as posing a significant security risk. However, airline industry stakeholders told us that while the rationale for exempting certain types of cargo from random inspection was understandable, the exemptions may have created potential security risks and vulnerabilities. Partly on the basis of a recommendation we made, TSA is evaluating existing exemptions to determine whether they pose a security risk and has reduced some exemptions that were previously allowed. We also noted that TSA had not developed performance measures to determine to what extent air carriers and indirect air carriers were complying with security requirements and had not analyzed the results of inspections to systematically target future inspections on those entities that pose a higher security risk to the domestic air cargo system. We have reported that without these performance measures and systematic analyses, TSA would be limited in its ability to effectively target its workforce for future inspections and fulfill its oversight responsibilities for this essential area of aviation security. With regard to inbound air cargo, in April 2007, we reported that TSA issued its air cargo security rule in May 2006, which included a number of provisions aimed at enhancing the security of inbound air cargo. For example, the final rule acknowledged that TSA amended its security directives and programs to triple the percentage of cargo inspected on domestic and foreign passenger aircraft. To implement the requirements contained in the air cargo security rule, TSA drafted revisions to its | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | existing security programs for domestic and foreign passenger air carriers and created new security programs for domestic and foreign all-cargo carriers. However, we reported that TSA requirements continue to allow inspection exemptions for certain types of inbound air cargo transported on passenger air carriers. We reported that this risk was further heightened because TSA has limited information on the background of and security risk posed by foreign shippers whose cargo may fall within these exemptions. TSA officials stated that the agency is holding discussions with industry stakeholders to determine whether additional revisions to current air cargo inspection exemptions are needed. We also reported that TSA inspects domestic and foreign passenger air carriers with service to the United States to assess whether the air carriers are complying with air cargo security requirements, such as inspecting a certain percentage of air cargo. We reported, however, that TSA did not currently inspect all air carriers transporting cargo into the United States. While TSA's compliance inspections provide useful information, the agency has not developed an inspection plan that includes performance goals and measures to determine to what extent air carriers are complying with security requirements. For more information, see GAO-06-76 and GAO-07-660.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to develop and implement procedures for screening air cargo. DHS noted that because the Aviation and Transportation Security Act set specific milestones for screening cargo and baggage carried on passenger aircraft, TSA focused initially on passenger aircraft. DHS issued the Air Cargo Security Requirements Final Rule in May 2006 that requires airports that currently maintain a Security Identification Display Area to expand the area to air cargo operating areas. At airports where a Security Identification Display Area is nonexistent but all-cargo operations occur, TSA requires aircraft operators to incorporate other security measures, such as security threat assessments for all persons with unescorted access to cargo, into their programs. TSA also reported that as of March 2007, it had 300 inspectors dedicated solely to oversight of the air cargo supply chain. During 2006, TSA reported that inspectors conducted more than 31,000 compliance reviews of air carriers and freight consolidators and have conducted covert testing of the domestic air cargo supply chain. TSA also reported that it is developing an air cargo risk-based targeting system to assess the risk of cargo to be moved on all aircraft operating within the United States.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed and implemented procedures to screen domestic and inbound air cargo. Furthermore, TSA has significantly increased the number of domestic air cargo inspections conducted of air carrier and indirect air carrier compliance with security requirements. However, as we previously reported, TSA requirements continue to allow inspection exemptions for certain types of inbound air cargo transported on passenger air carriers, which could create security vulnerabilities, and TSA has limited information on the background of and security risk posed by foreign shippers whose cargo may fall within these exemptions. | |
| 24. Develop and implement technologies to screen air cargo | *GAO findings:* DHS has not yet developed and implemented technologies needed to screen air cargo. TSA's plans for enhancing air cargo security include developing and testing air cargo inspection technology. However, these planned enhancements may pose operational, financial, and technological challenges to the agency and air cargo industry stakeholders. In October 2005 we reported that TSA had completed a pilot program focused on testing the applicability of EDS technology to inspect individual pieces of air cargo, referred to as break bulk cargo. Although EDS is an approved method for inspecting passenger baggage, it had not been tested by TSA to determine its effectiveness in inspecting air cargo. According to TSA officials, TSA must review the results of its EDS pilot test before the agency would determine whether to certify EDS for inspecting air cargo. According to TSA officials, the agency has also been pursuing multiple technologies to automate the detection of explosives in the types and quantities that would cause catastrophic damage to an aircraft in flight. TSA planned to develop working prototypes of these technologies by September 2006 and complete operational testing by 2008. TSA acknowledged that full development of these technologies may take 5 to 7 years. In April 2007, we reported that DHS has taken some steps to incorporate new technologies into strengthening the security of air | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | cargo, which will affect both domestic and inbound air cargo. However, we reported that TSA and DHS's Science and Technology Directorate were in the early stages of evaluating available aviation security technologies to determine their applicability to the domestic air cargo environment. TSA and the Science and Technology Directorate are seeking to identify and develop technologies that can effectively inspect and secure air cargo with minimal impact on the flow of commerce. According to TSA officials, there is no single technology capable of efficiently and effectively inspecting all types of air cargo for the full range of potential terrorist threats, including explosives and weapons of mass destruction. Accordingly, TSA, together with the Science and Technology Directorate, is conducting a number of pilot programs that are testing a variety of different technologies that may be used separately or in combination to inspect and secure air cargo. These pilot programs seek to enhance the security of air cargo by improving the effectiveness of air cargo inspections through increased detection rates and reduced false alarm rates, while addressing the two primary threats to air cargo identified by TSA—hijackers on an all-cargo aircraft and explosives on passenger aircraft. TSA anticipates completing its pilot tests by 2008, but has not yet established time frames for when it might implement these methods or technologies for the inbound air cargo system. According to DHS and TSA officials, further testing and analysis will be necessary to make determinations about the capabilities and costs of these technologies when employed for inspecting inbound air cargo at foreign locations. For more information, see GAO-06-76 and GAO-07-660.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to develop and implement air cargo screening technologies. TSA reported that new technologies to physically screen air cargo will not be available in the near term. TSA reported that it is using and improving existing technologies to screen air cargo. For example, TSA reported increasing the use of canine teams and stated that these teams dedicate about 25 percent of their time of air cargo security activities.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS focused initial aviation security efforts on fulfilling congressional mandates related to passenger and baggage screening and has faced challenges in its efforts to develop and implement air cargo screening technologies. In prior work, we reported that TSA has taken actions to develop technologies for screening air cargo, but had not yet tested the effectiveness of various technologies in inspecting air cargo. We also reported that full development of technologies for screening air cargo may be years away. | |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken a sufficient number of actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

[a] The terms “inspecting” and “screening” have been used interchangeably by TSA to denote some level of examination of a person or good, which can entail a number of different actions, including manual physical inspections to ensure that cargo does not contain weapons, explosives, or stowaways, or inspections using nonintrusive technologies that do not require the cargo to be opened in order to be inspected. For this and the subsequent performance expectation, we use the term “screen” to refer to this broad range of activities. However, in our April 2007 report that is referenced in this performance expectation’s associated findings section, the term “screening” was used when referring to TSA or CBP efforts to apply a filter to analyze cargo related information to identify cargo shipment characteristics or anomalies for security risks. The term “inspection” was used to refer only to air carrier, TSA, or CBP efforts to examine air cargo through physical searches and the use of nonintrusive technologies.

## DHS Has Made Moderate Progress in Securing Surface Transportation Modes

DHS has undertaken various initiatives to secure surface transportation modes, and within the department, TSA is primarily responsible for surface transportation security efforts. Since its creation following the events of September 11, 2001, TSA has focused much of its efforts and resources on meeting legislative mandates to strengthen commercial aviation security. However, TSA has more recently placed additional focus on securing surface modes of transportation, which includes establishing security standards and conducting assessments and inspections of surface transportation modes such as passenger and freight rail; mass transit; highways, including commercial vehicles; and pipelines. Although TSA has primary responsibility within the department for surface transportation security, the responsibility for securing rail and other transportation modes is shared among federal, state, and local governments and the private sector. For example, with regard to passenger rail security, in addition to TSA, DHS’s Office of Grant Programs provides grant funds to rail operators and conducts risk assessments for passenger rail agencies. Within the Department of Transportation, the Federal Transit Administration and Federal Railroad Administration have responsibilities for passenger rail safety and security. In addition, public and private passenger rail operators are also responsible for securing their rail systems.

As shown in table 24, we identified five performance expectations for DHS in the area of surface transportation security, and we found that overall DHS has made moderate progress in meeting those performance expectations. Specifically, we found that DHS has generally achieved three of these performance expectations and has generally not achieved two others.

Table 24: Performance Expectations and Progress Made in Surface Transportation Security

| | Assessment | | |
|---|---|---|---|
| Performance expectation | Generally achieved | Generally not achieved | No assessment made |
| 1. Develop and adopt a strategic approach for implementing surface transportation security functions | ✓ | | |
| 2. Conduct threat, criticality, and vulnerability assessments of surface transportation assets | ✓ | | |
| 3. Issue standards for securing surface transportation modes | | ✓ | |
| 4. Conduct compliance inspections for surface transportation systems | | ✓ | |
| 5. Administer grant programs for surface transportation security | ✓ | | |
| **Total** | **3** | **2** | **0** |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

Table 25 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of surface transportation security and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation's key elements (generally not achieved).

Table 25: Performance Expectations and Assessment of DHS Progress in Surface Transportation Security

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Develop and adopt a strategic approach for implementing surface transportation security functions | *GAO findings:* DHS has developed a strategic approach for securing surface transportation modes, which include mass transit, passenger rail, freight rail, commercial vehicles, pipelines, and related infrastructure such as roads and highways. In the past we have reported that TSA had not issued the Transportation Sector Specific Plan or supporting plans for securing all modes of transportation, in accordance with DHS's National Infrastructure Protection Plan and a December 2006 executive order. We reported that until TSA issued the sector-specific plan and supporting plans, it lacked a clearly communicated strategy with goals and objectives for securing the transportation sector. In addition, in March 2007, we testified that as of September 2005, DHS had begun developing, but had not yet completed a framework to help federal agencies and the private sector develop a consistent approach for analyzing and comparing risks to transportation and other critical sectors. For more information, see *Passenger Rail Security: Enhanced Leadership Needed to Prioritize and Guide Security Efforts,* GAO-07-225T and *Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts,* GAO-07-583T.<br>*DHS updated information:* In May 2007, DHS issued the sector-specific plan for transportation systems and supporting annexes for surface transportation assets, and reported taking actions to adopt the strategic approach outlined by the plan. The Transportation Systems Sector-Specific Plan and its supporting modal implementation plans and appendixes establish a strategic approach based on the National Infrastructure Protection Plan and Executive Order 13416, Strengthening Surface Transportation Security. The Transportation Systems Sector-Specific Plan describes the security framework that is intended to enable sector stakeholders to make effective and appropriate risk-based security and resource allocation decisions. The key efforts to be undertaken according to the plan include the (1) identification of assets, systems, networks and functions to be protected; (2) assessment of risks; (3) prioritization of risk management options; (4) development and implementation of security programs; (5) measurement of progress; (6) assessment and prioritization of research and development investments; and (7) management and coordination of sector responsibilities, including the sharing of information. In addition, during the course of our ongoing work assessing mass transit, freight rail, commercial vehicles, and highway infrastructure, we identified that DHS has begun to implement some of the security initiatives outlined in the sector-specific plan for transportation systems and supporting annexes.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation because TSA has issued the Transportation Sector-Specific Plan and supporting plans, a significant step in its efforts to develop and adopt a strategic approach for surface transportation security functions. While DHS has issued a strategy for securing all transportation modes, and has demonstrated that it has begun to take actions to implement the goals and objectives outlined in the strategy, we have not yet analyzed the overall quality of the plan or supporting modal annexes, the extent to which efforts outlined in the plans and annexes were implemented, or the effectiveness of identified security initiatives. The four performance expectations in the surface transportation security mission area discussed below are generally related to DHS's implementation of the strategy. In addition, we recognize that the acceptance of DHS's approach by federal, state, local, and private sector stakeholders is crucial to its successful implementation. However, we have not assessed the extent to which the plan and supporting modal annexes were coordinated with or adopted by these stakeholders. We will continue to assess DHS' efforts to implement its strategy for securing surface transportation modes as part of our ongoing reviews of mass transit, freight rail, commercial vehicles, and highway infrastructure security. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 2. Conduct threat, criticality, and vulnerability assessments of surface transportation assets | *GAO findings:* DHS has taken actions to conduct threat, criticality, and vulnerability assessments of some surface transportation assets, particularly passenger and freight rail, but has not provided us with evidence that it has completed assessments in other surface transportation modes. In 2005, we reported that DHS and TSA conducted threat and vulnerability assessments of passenger rail systems. More recently, we testified that TSA had reported completing an overall threat assessment for mass transit, passenger, and freight rail modes and had conducted criticality assessments of nearly 700 passenger rail stations. In addition, in March 2007 we testified that DHS's Office of Grants and Training, now called the Office of Grant Programs, developed and implemented a risk assessment tool to help passenger rail operators better respond to terrorist attacks and prioritize security measures. Passenger rail operators must have completed a risk assessment to be eligible for financial assistance through the fiscal year 2007 Transit Security Grant Program, which includes funding for passenger rail. To receive grant funding, rail operators are also required to have a security and emergency preparedness plan that identifies how the operator intends to respond to security gaps identified by risk assessments. As of February 2007, DHS had completed or planned to conduct risk assessments of most passenger rail operators. According to rail operators, DHS's risk assessment process enabled them to prioritize investments on the basis of risk and allowed them to target and allocate resources toward security measures that will have the greatest impact on reducing risk across their rail systems. However, TSA has not provided us with evidence that it has yet conducted threat and vulnerability assessments of all 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. Until threat, criticality, and vulnerability assessments have been coordinated and completed, and until TSA determines how to use the results of these assessments to analyze and characterize risk, it may not be possible to effectively prioritize passenger rail assets and guide investment decisions about protecting them. TSA has reported conducting additional risk assessments in rail and other transportation modes since the issuance of our September 2005 report. We will review these assessments and other TSA efforts to secure surface transportation modes in our ongoing and planned work related to passenger and freight rail, highway infrastructure, and commercial vehicle security. For more information, see GAO-07-225T; *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts,* GAO-06-181T; and *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts,* GAO-05-851.<br>*DHS updated information:* In March and April 2007, and as part of ongoing work assessing freight rail, commercial vehicles, and highway infrastructure, DHS provided us with updated information on its efforts to conduct threat, criticality, and vulnerability assessments for surface transportation assets. With regard to threat assessments, DHS receives and uses threat information as part of its surface transportation security efforts. TSA's Office of Intelligence provides annual intelligence summaries, periodic updates, and other current intelligence briefings to the rest of TSA. The annual assessments are shared with TSA stakeholders, and TSA provided us copies for all transportation modes. With regard to criticality assessments, DHS has conducted such assessments for some surface transportation modes. For example, TSA has conducted Corporate Security Reviews with 38 state Department of Transportation highway programs. For commercial vehicles, TSA has conducted 32 Corporate Security Reviews with large motor carriers, in an industry with over one million firms. It has also completed a pilot program with the state of Missouri to supplement the state's regular safety inspections of trucking firms with Corporate Security Reviews. TSA reports that over 1,800 Corporate Security Reviews have been completed in Missouri as part of this program. In addition, the National Protection and Programs Directorate Infrastructure Protection conducts highway infrastructure assessments that look at tier one and tier two critical highway infrastructure. The National Protection and Programs Directorate completed 54 highway infrastructure assessments performed from 2004 through May 2007. With regard to vulnerability assessments, DHS has conducted such assessments for surface transportation | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | modes. For example, TSA reported that its Security Analysis and Action Program utilizes several different tools to identify vulnerabilities based on specific scenarios, such as an improvised explosive device on a passenger train. The purpose of the program is to gather information, identify generally accepted best practices, and benchmark existing security operations in comparison to established industry security practices. According to TSA, among other things, the Security Analysis and Action Program creates a baseline for future multimodal security assessments, develops a road map for future passenger rail security evaluations, and helps prioritize security countermeasures and emergency response enhancement needs based on threats and risks. For freight rail, we found that TSA has conducted vulnerability assessments of High Threat Urban Area rail corridors where toxic inhalation hazard shipments are transported. TSA reported that these corridor assessments provide site-specific mitigation strategies and lessons learned as well as tactics that can be modified for use at the corporate or national level. Furthermore, TSA reported that its Visible Intermodal Prevention and Protection Teams are deployed randomly to prepare for emergency situations in which TSA assets would be invited to assist a local transit agency. According to TSA, these teams allow TSA and local entities to develop templates that can be implemented in emergency situations and to supplement existing security resources. As of March 20, 2007, TSA reported that 50 Visible Intermodal Prevention and Protection team exercises have been conducted at various mass transit and passenger rail systems since December 2005. In addition, TSA reported that through its Pipeline Security Division, it has conducted 63 Corporate Security Reviews, on-site reviews of pipeline companies' security planning. The goals of these reviews are to develop knowledge of security planning and execution at pipeline sites; establish and maintain working relationships with pipeline security personnel; and identify and share security practices.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has taken actions to conduct threat, criticality, and vulnerability assessments in surface transportation sectors, but we have not yet reviewed the quality of many of these assessments. DHS uses threat assessments and information as part of its surface transportation security efforts and has used criticality assessments to help prioritize its efforts. DHS has also conducted vulnerability assessment of assets within surface transportation modes, particularly for mass transit, freight rail, and highway infrastructure. However, with regard to High Threat Urban Area rail corridor assessments, DHS has not yet fully designated those corridors for which it plans to conduct future assessments. Moreover, for commercial vehicles and highway infrastructure, DHS has not yet completed all planned vulnerability assessments. | |
| 3. Issue standards for securing surface transportation modes | *GAO findings:* DHS has initiated efforts to develop security standards for surface transportation modes, but DHS did not provide us with information on its efforts beyond passenger and freight rail. In 2006, TSA was planning to issue security standards for all modes of transportation. TSA planned to issue only a limited number of standards—that is, standards will be issued only when assessments of the threats, vulnerabilities, and criticality indicate that the level of risk is too high or unacceptable. TSA has developed security directives and security action items—recommended measures for passenger rail operators to implement in their security programs to improve both security and emergency preparedness—for passenger rail and issued a proposed rule in December 2006 on passenger and freight rail security requirements. For more information, see GAO-07-225T; GAO-06-181T; and GAO-05-851.<br>*DHS updated information:* In April 2007, and as part of ongoing work, DHS provided us with updated information on TSA's efforts to issue standards for securing surface transportation modes. According to DHS, TSA uses field activities to assess compliance with security directives and implementation of noncompulsory security standards and protective measures with the objective of a broad-based enhancement of passenger rail and rail transit security. Through the Baseline Assessment for Security Enhancement inspectors review implementation by mass transit and passenger rail systems of the 17 Security and Emergency Management Action Items (security action items) that TSA and the Federal Transit Administration jointly developed, in coordination with the Mass Transit Sector Coordinating | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | Council. This initiative aims to elevate security posture throughout the mass transit and passenger rail mode by implementation of baseline security measures adaptable to the operating circumstances of any system. TSA also reported that in December 2006, it issued a notice of proposed rulemaking on new security measures for freight rail carriers designed to ensure 100 percent positive handoff of toxic inhalation hazard shipments that enter high threat urban areas and establish security protocols for custody transfers of toxic inhalation hazard rail cars in high-threat urban areas. TSA also reported that its High Threat Urban Area rail corridor assessments supported the development of the Recommended Security Action Items for the Rail Transportation of Toxic Inhalation Materials issued by DHS and the Department of Transportation in June 2006.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has taken actions to develop and issue surface transportation security standards for passenger and freight rail modes. However, DHS did not provide us with evidence of its efforts to develop and issue security standards for all surface transportation modes or a rationale or explanation why standards may not be needed for other modes. | |
| 4. Conduct compliance inspections for surface transportation systems | *GAO findings:* DHS has made progress in conducting compliance inspections, particularly in hiring and deploying inspectors, but inspectors' roles and missions have not yet been fully defined. TSA officials stated the agency has hired 100 surface transportation inspectors whose stated mission is to, among other duties, monitor and enforce compliance with TSA's rail security directives. However, some passenger rail operators have expressed confusion and concern about the role of TSA's inspectors and the potential that TSA inspections could be duplicative of other federal and state rail inspections. TSA rail inspector staff stated that they were committed to avoiding duplication in the program and communicating their respective roles to rail agency officials. According to TSA, since the initial deployment of surface inspectors, these inspectors have developed relationships with security officials in passenger rail and transit systems, coordinated access to operations centers, participated in emergency exercises, and provided assistance in enhancing security. However, the role of inspectors in enforcing security directives has not been fully defined. We will continue to assess TSA's compliance efforts during follow-on reviews of surface transportation modes For more information, see GAO-07-225T; GAO-06-181T; and GAO-05-851.<br>*DHS updated information:* In March and April 2007, and as part of ongoing reviews, DHS provided us with updated information on its efforts to conduct compliance inspections for surface transportation systems. For example, with regard to freight rail, TSA reported visiting terminal and railroad yards to measure implementation of 7 of 24 recommended security action items for the rail transportation of toxic inhalation hazard materials. TSA reported that during the end of 2006, its inspectors visited about 150 individual railroad facilities. Through its Surface Transportation Security Inspection program, TSA reported that its inspectors conduct inspections of key facilities for rail and transit systems to assess transit systems' implementation of core transit security fundamentals and comprehensive security action items; conduct examinations of stakeholder operations, including compliance with security directives; identify security gaps; and develop effective practices. TSA noted that its field activities also assess compliance with security directives and implementation of noncompulsory security standards and protective measures. For example, TSA reported that through the Baseline Assessment for Security Enhancements program, inspectors review mass transit and passenger rail systems' implementation of the 17 Security and Emergency Management Action Items jointly developed by TSA and the Federal Transit Administration. The program is a means to establish baseline security program data applicable to all surface mass transit systems. TSA also noted that it deploys inspectors to serve as federal liaisons to mass transit and passenger rail system operations centers and provide other security support and assistance in periods of heightened alert or in response to security incidents.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | expectation. DHS has taken steps to conduct compliance inspections for surface transportation systems and has made progress in hiring and deploying inspectors. Although DHS has deployed inspectors to conduct compliance inspections and carry out other security activities in the mass transit (mass transit includes passenger rail) and freight rail modes, DHS did not provide us with evidence that it has conducted compliance inspections for other surface transportation modes or information on whether the department believes compliance inspections are needed for other modes. Moreover, we reported that the role of inspectors in enforcing security requirements has not been fully defined, and DHS did not provide us with documentation on its efforts to better define these roles. | |
| 5. Administer grant programs for surface transportation security | *GAO findings:* In March 2007, we reported that the DHS Office of Grants and Training, now called the Office of Grant Programs, has used various programs to fund passenger rail security since 2003. Through the Urban Area Security Initiative grant program, the Office of Grants and Training has provided grants to urban areas to help enhance their overall security and preparedness level to prevent, respond to, and recover from acts of terrorism. In 2003 and 2004, $65 million and $50 million, respectively, were provided to rail transit agencies through the Urban Area Security Initiative program. In addition, the 2005 DHS appropriations action provided $150 million for intercity passenger rail transportation, freight rail, and transit security grants. In fiscal year 2006, $150 million was appropriated, and in fiscal year 2007 $175 million was appropriated for the same purposes. The Office of Grants and Training used this funding to build on the work under way through the Urban Area Security Initiative program and create and administer new programs focused specifically on transportation security, including the Transit Security Grant Program and the Intercity Passenger Rail Security Grant Program. During fiscal year 2006, the Office of Grants and Training provided $110 million to passenger rail transit agencies through the Transit Security Grant Program and about $7 million to Amtrak through the Intercity Passenger Rail Security Grant Program. During fiscal year 2007, the Office of Grants and Training plans to distribute $156 million for rail and bus security grants and $8 million to Amtrak. In January 2007, the Office of Grants and Training reported that the Intercity Passenger Rail Security Program had been incorporated into the Transit Security Grant Program. We reported that although the Office of Grants and Training has distributed hundreds of millions of dollars in grants to improve passenger rail security, issues have surfaced about the grant process. For example, we reported that as DHS works to refine its risk assessment methodologies, develop better means of assessing proposed investments using grant funds, and align grant guidance with the implementation of broader emergency preparedness goals, such as implementation of the National Preparedness Goal, it has annually made changes to the guidance for the various grants it administers. These changes include changes in the eligibility for grants. As a result of these annual changes, awardees and potential grant recipients must annually review and understand new information on the requirements for grant applications including justification of their proposed use of grant funds. We also reported that funds awarded through the Transit Security Grant Program can be used to supplement funds received from other grant programs. However, allowable uses are not clearly defined. For example, Transit Security Grant Program funds can be used to create canine teams but cannot be used to maintain these teams—that is, the grant funds cannot be used for food, medical care, and other such maintenance costs for the dogs on the team. Grant recipients have expressed a need for clear guidance on the allowable use of grants and how they can combine funds from more than one grant to fund and implement specific projects. . In addition, some industry stakeholders have raised concerns regarding DHS's current grant process, noting that there are time delays and other barriers in grant funding reaching owners and operators of surface transportation assets. We will be assessing grants for mass transit as part of our ongoing work. For more information, see GAO-06-181T and *Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts,* GAO-07-583T.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | grant programs for surface transportation security. For example, TSA considers various factors in Transit Security Grant Program proposals, including the enhancement of capabilities to (1) deter, detect, and respond to terrorist attacks employing improvised explosive devices; (2) mitigate high-consequence risks identified in individual transit system risk assessments; (3) implement technology for detection of explosives and monitoring for suspicious activities; (4) improve coordination with law enforcement and emergency responders; and (5) expand security training and awareness among employees and passengers. TSA reported using the Transit Security Grant Program to drive improvements in areas such as training for key personnel, drills, exercises, and public awareness and preparedness.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed and administered grant programs for various surface transportation modes. However, some industry stakeholders have raised concerns regarding DHS's current grant process, such as time delays and other barriers in the provision of grant funding. We have not yet assessed DHS's provision of grant funding or the extent to which DHS monitors use of the funds. A recent legislative proposal would have the Department of Transportation, rather than DHS, distribute grant funds for specified surface transportation security purposes. | |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

## DHS Has Made Substantial Progress in Maritime Security

DHS has undertaken various programs to secure the maritime sector. In general, these maritime security programs fall under one of three areas—port and vessel security, maritime intelligence, and maritime supply chain security. Within DHS, various component agencies are responsible for maritime security efforts, including the Coast Guard, CBP, TSA, and the Domestic Nuclear Detection Office. The Coast Guard is responsible for port facility inspections and has lead responsibility in coordinating maritime information sharing efforts. CBP is responsible for addressing the threat posed by terrorist smuggling of weapons in oceangoing containers. TSA is responsible for the implementation of the transportation worker identification credential program. The Domestic Nuclear Detection Office is responsible for acquiring and supporting the deployment of radiation detection equipment, including portal monitors, within the United States.

As shown in table 26, we identified 23 performance expectations for DHS in the area of maritime security, and we found that overall DHS has made substantial progress in meeting those expectations. Specifically, we found that DHS has generally achieved 17 performance expectations and has generally not achieved 4 others. For 2 performance expectations, we did not make an assessment.

Table 26: Performance Expectations and Progress Made in Maritime Security

| Performance expectation | Assessment | | |
|---|---|---|---|
| | Generally achieved | Generally not achieved | No assessment made |
| 1. Develop national plans for maritime security | ✓ | | |
| 2. Develop national plans for maritime response | ✓ | | |
| 3. Develop national plans for maritime recovery | ✓ | | |
| 4. Develop regional (port-specific) plans for security | ✓ | | |
| 5. Develop regional (port-specific) plans for response | ✓ | | |
| 6. Develop regional (port-specific) plans for recovery | | ✓ | |
| 7. Ensure port facilities have completed vulnerability assessments and developed security plans | ✓ | | |
| 8. Ensure that vessels have completed vulnerability assessments and developed security plans | ✓ | | |
| 9. Exercise security, response, and recovery plans with key maritime stakeholders to enhance security, response, and recovery efforts | ✓ | | |
| 10. Implement a national facility access control system for port secured areas | | ✓ | |
| 11. Implement a port security grant program to help facilities improve their security capabilities | ✓ | | |
| 12. Develop a national plan to establish and improve maritime intelligence | | | ✓ |
| 13. Establish operational centers to monitor threats and fuse intelligence and operations at the regional/port level | ✓ | | |
| 14. Collect information on incoming ships to assess risks and threats | ✓ | | |
| 15. Develop a vessel-tracking system to improve intelligence and maritime domain awareness on vessels in U.S. waters | ✓ | | |
| 16. Develop a long-range vessel-tracking system to improve maritime domain awareness | | ✓ | |
| 17. Collect information on arriving cargo for screening purposes | ✓ | | |
| 18. Develop a system for screening and inspecting cargo for illegal contraband | ✓ | | |

|  | Assessment |  |  |
|---|---|---|---|
| Performance expectation | Generally achieved | Generally not achieved | No assessment made |
| 19. Develop a program to screen incoming cargo for radiation |  | ✓ |  |
| 20. Develop a program to work with foreign governments to inspect suspicious cargo before it leaves for U.S. ports | ✓ |  |  |
| 21. Develop a program to work with the private sector to improve and validate supply chain security | ✓ |  |  |
| 22. Develop standards for cargo containers to ensure their physical security |  |  | ✓ |
| 23. Develop an international port security program to assess security at foreign ports | ✓ |  |  |
| **Total** | **17** | **4** | **2** |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

Table 27 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of maritime security and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation's key elements (generally not achieved).

Table 27: Performance Expectations and Assessment of DHS Progress in Maritime Security

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Develop national plans for maritime security | *GAO findings:* The President and the Secretaries of Homeland Security, Defense, and State approved the supporting plans for National Strategy for Maritime Security in October 2005. The National Strategy for Maritime Security has eight supporting plans that are intended to address the specific threats and challenges of the maritime environment. The supporting plans are the National Plan to Achieve Domain Awareness; the Global Maritime Intelligence Integration Plan; the Maritime Operational Threat Response Plan; the International Outreach and Coordination Strategy; the Maritime Infrastructure Recovery Plan; the Maritime Transportation System Security Plan; the Maritime Commerce Security Plan; and the Domestic Outreach Plan. In addition, in September 2005, the Coast Guard issued Maritime Sentinel. Maritime Sentinel provides a framework for the Coast Guard's Ports, Waterways and Coastal Security program, setting out the Coast Guard's mission and goals in that area. Our review of Maritime Sentinel showed that the plan is results-oriented with outcome-based goals but that it needs to better describe the human capital resources necessary to achieve them.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to develop national plans for maritime security. DHS reported that the Coast Guard has issued a number of plans supporting or relating to maritime security.<br>*Our assessment:* Based on our review of Maritime Sentinel and updated information DHS provided, we conclude that that DHS has generally achieved this expectation. | Generally achieved |
| 2. Develop national plans for maritime response | *GAO findings:* DHS has developed a national plan for response in conjunction with the Department of Defense. We have reported that the Maritime Operational Threat Response Plan establishes roles and responsibilities for responding to marine terrorism to help resolve jurisdictional issues among responding agencies. For more information, see *Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention*, GAO-05-170.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to develop national plans for maritime response. For example, DHS reported that the Maritime Operational Threat Response Plan is a strategic plan that addresses the full range of maritime threats including terrorism, piracy, drug smuggling, migrant smuggling, weapons of mass destruction proliferation, maritime hijacking, and fisheries incursions. DHS stated that this interagency national plan supersedes Presidential Directive-27 (in the maritime domain only) for addressing nonmilitary incidents of national security significance and has been successfully exercised numerous times among agencies, including actual effective threat resolution. DHS further stated that the Maritime Operational Threat Response Plan is a national-level process to achieve consistently coordinated action and desired outcomes that directly support National Security Presidential Directive-41/Homeland Security Presidential Directive-13.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation as DHS has developed the Maritime Operational Threat Response Plan, which details agency responsibilities during incidents of marine terrorism. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 3. Develop national plans for maritime recovery | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation, as DHS has developed the Maritime Infrastructure Recovery Plan, and the plan establishes a framework for maritime recovery. In April 2006, DHS released the Maritime Infrastructure Recovery Plan. The Maritime Infrastructure Recovery Plan is intended to facilitate the restoration of maritime commerce after a terrorist attack or natural disaster and reflects the disaster management framework outlined in the National Response Plan. The Maritime Infrastructure Recovery Plan addresses issues that should be considered by ports when planning for natural disasters. However, it does not set forth particular actions that should be taken at the port level, leaving those determinations to be made by the port operators themselves. For more information, see *Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery*, GAO-07-412. | Generally achieved |
| 4. Develop regional (port-specific) plans for security | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed regional (port-specific) plans for security. The Coast Guard led efforts to conduct a security assessment of each of the nation's seaports and develop a security plan for each seaport zone. Under regulations implementing the Maritime Transportation Security Act, a Coast Guard Captain of the Port must develop an area plan in consultation with an Area Maritime Security Committee. These committees are typically composed of members from federal, local, and state governments; law enforcement agencies; maritime industry and labor organizations; and other port stakeholders that may be affected by security policies. In April 2007 we reported that implementing regulations for the Maritime Transportation Security Act specified that area plans include, among other things, operational and physical security measures in place at the port under different security levels, details of the security incident command and response structure, procedures for responding to security threats including provisions for maintaining operations in the port, and procedures to facilitate the recovery of the marine transportation system after a security incident. A Coast Guard Navigation and Vessel Inspection Circular provided a common template for area plans and specified the responsibilities of port stakeholders under the plans. Currently, 46 area plans are in place at ports around the country. For more information, see *Maritime Security: Observations on Selected Aspects of the SAFE Port Act,* GAO-07-754T; *Coast Guard: Observations on Agency Performance, Operations and Future Challenges,* GAO-06-448T; *Maritime Security: Enhancements Made, but Implementation and Sustainability Remain Key Challenges,* GAO-05-448T; and *Maritime Security: Better Planning Needed to Help Ensure an Effective Port Security Assessment Program,* GAO-04-1062. | Generally achieved |
| 5. Develop regional (port-specific) plans for response | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed regional (port-specific) plans for response. We have reported that the Captain of the Port is responsible for establishing both spill and terrorism response plans. In doing so, the Captain of the Port must identify local public and private port stakeholders who will develop and revise separate plans for marine spills of oil and hazardous materials and for terrorism response. Both plans call for coordinated implementation with other plans, such as the response and security plans developed by specific facilities or vessels. At the port level, effectively integrating spill and terrorism emergency responses requires all plans to operate in unison—the port spill response plan and the port terrorism response plan, as well as facility and vessel response plans. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 6. Develop regional (port-specific) plans for recovery | *GAO findings:* DHS has generally not developed regional (port-specific) plans for recovery. We have reported that guidance in the Maritime Infrastructure Recovery Plan suggests that ports develop priorities for bringing vessels into port after a closure. Additionally, port terrorism response plans must include a section on crisis management and recovery to ensure the continuity of port operations.<br>*DHS updated information:* In April 2007, DHS provided us with updated information on its efforts to develop regional (port-specific) plans for recovery. DHS reported that the Coast Guard and CBP have developed protocols for recovery and resumption of trade. DHS stated that these protocols are currently being discussed with other federal agencies for coordination purposes and with the private sector to ensure that federal activities facilitate private sector recovery efforts. DHS also reported that Coast Guard headquarters is preparing guidance for field units for including recovery in their plans for creating Maritime Transportation System Recovery Units at the local (sector) level. Further, DHS reported that several ports have included recovery as part of their area plans, such as all ports in the Coast Guard's Atlantic Area, the Ports of Los Angeles and Long Beach, and San Francisco. DHS stated that the level of detail in these plans varies but noted that many are working to enhance the section on recovery and resumption of trade. DHS added that these plans are developing as all-hazard plans to include both natural and man-made incidents.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Our prior work has shown that work remains in DHS's efforts to develop regional (port-specific) plans for recovery. | Generally not achieved |
| 7. Ensure port facilities have completed vulnerability assessments and developed security plans | *GAO findings:* DHS has taken steps to ensure that port facilities have completed vulnerability assessments and developed security plans. Maritime Transportation Security Act implementing regulations require designated owners or operators of maritime facilities to identify vulnerabilities and develop security plans for their facilities. In May 2005 we reported that the Coast Guard had reviewed and approved the security plans of the over 3,000 facilities that were required to identify their vulnerabilities and take action to reduce them. Six months after July 1, 2004, the date by which the security plans were to be implemented, the Coast Guard reported that it had completed on-site inspections of all facilities to ensure the plans were being implemented as approved. In April 2007 we reported that Coast Guard guidance calls for the Coast Guard to conduct on-site facility inspections to verify continued compliance with security plans on an annual basis. A Security and Accountability for Every (SAFE) Port Act amendment to the Maritime Transportation Security Act requires the Coast Guard to conduct at least two inspections of each facility annually, and it required that one of these inspections be unannounced. We are currently conducting a review of the Coast Guard's efforts for ensuring facilities' compliance with various Maritime Transportation Security Act requirements. For more information, see GAO-07-754T; GAO-05-448T; and *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security,* GAO-04-838.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to ensure that port facilities have completed vulnerability assessments and developed security plans. DHS reported that its Alternative Security Program allows for participants to use templates pre-approved by the Coast Guard for developing their security plans. Facilities that use these plans then undergo security plan verifications, as required by the Maritime Transportation Security Act.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has made progress in ensuring that port facilities have completed vulnerability assessments and developed security plans. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 8. Ensure that vessels have completed vulnerability assessments and developed security plans | *GAO findings:* DHS has made progress in ensuring that vessels have done vulnerability assessments and developed security plans. In May 2005 we reported that the Coast Guard had reviewed and approved the security plans of the more than 9,000 vessels that were required to identify their vulnerabilities and take action to reduce them. Six months after July 1, 2004, the date by which the security plans were to be implemented, the Coast Guard reported that it had completed on-site inspections of thousands of vessels to ensure the plans were being implemented as approved. For more information, see *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security*, GAO-04-838 and GAO-05-448T.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to ensure that vessels have completed vulnerability assessments and developed security plans. DHS reported that the Coast Guard completed security plan verifications for all inspected U.S.-flagged vessels by July 2005. DHS further reported that to date, the Coast Guard has completed security plan verifications on 98 percent of uninspected U.S.-flagged vessels regulated in accordance with the Maritime Transportation Security Act. DHS noted that uninspected vessels are not required to undergo security plan verifications exams by regulation but stated the Coast Guard was committed to the goal of encouraging all vessel owners of uninspected vessels to undergo such examinations on a voluntary basis by the end of 2006.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has taken steps to ensure that vessels have completed vulnerability assessments and developed security plans. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 9. Exercise security, response, and recovery plans with key maritime stakeholders to enhance security, response, and recovery efforts | *GAO findings:* DHS has generally exercised security, response, and recovery plans (at least at the regional level) with key stakeholders. The Coast Guard has primary responsibility for such testing and evaluation in the nation's ports and waterways, and as part of its response, it has added multi-agency and multicontingency terrorism exercises to its training program. These exercises vary in size and scope and are designed to test specific aspects of the Coast Guard's terrorism response plans, such as communicating with state and local responders, raising maritime security levels, or responding to incidents within the port. For each exercise the Coast Guard conducts, an after-action report detailing the objectives, participants, and lessons learned must be produced. We reported in January 2005 on the issues identified in port security exercises. For example, we found that 59 percent of the exercises raised communications issues, and 28 percent raised concerns with participants' knowledge about who has jurisdiction or decision-making authority. In April 2007, we reported that the Coast Guard had conducted a number of exercises of its area plans over the past several years. For example, in fiscal year 2004, the Coast Guard conducted 85 port-based terrorism exercises that addressed a variety of possible scenarios. In August 2005, the Coast Guard and TSA initiated the Port Security Training Exercise Program—an exercise program designed to involve the entire port community, including public governmental agencies and private industry, and intended to improve connectivity of various surface transportation modes and enhance area plans. Between August 2005 and October 2007, the Coast Guard expects to conduct Port Security Training Exercise Program exercises for 40 area committees and other port stakeholders. For more information, see GAO-07-754T and *Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention,* GAO-05-170.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to exercise security, response, and recovery plans with key maritime stakeholders to enhance security, response, and recovery efforts. DHS reported that for each exercise the Coast Guard conducts, an after-action report detailing the objectives, participants, and lessons learned must be produced within 21 days for non-contract-supported exercises and within 81 days for contract-supported exercises.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has made progress in exercising security, response, and recovery plans with key maritime stakeholders to enhance security, response, and recovery efforts. | Generally achieved |
| 10. Implement a national facility access control system for port secured areas | *GAO and DHS IG findings:* While DHS has taken steps to provide for an effective national facility access control system at ports, significant challenges remain. In September 2006 we identified several major challenges DHS and industry stakeholders face in addressing problems identified during Transportation Worker Identification Credential program testing and ensuring that key components of the Transportation Worker Identification Credential program can work effectively in the maritime sector, such as ensuring that the access control technology required to operate the Transportation Worker Identification Credential program, such as biometric card readers, works effectively in the maritime sector. Further, stakeholders at all 15 Transportation Worker Identification Credential testing locations we visited told us that TSA did not effectively communicate and coordinate with them regarding any problems that arose during testing at their facility. In July 2006 the DHS IG found that significant security vulnerabilities existed relative to the Transportation Worker Identification Credential prototype systems, documentation, and program management. Further, the DHS IG reported that the Transportation Worker Identification Credential prototype systems were vulnerable to various internal and external security threats and that security-related issues identified could threaten the confidentiality, integrity, and availability of sensitive Transportation Worker Identification Credential data. In April 2007 we testified that DHS | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | had made progress toward implementing the Transportation Worker Identification Credential. We reported, for example, that DHS had issued a rule that sets forth the requirements for enrolling and issuing cards to workers in the maritime sector and developed a schedule for enrolling worker and issuing Transportation Worker Identification Credential cards at ports. | |
| | In April 2007 we reported that the SAFE Port Act contained a requirement for implementing the first major phase of the Transportation Worker Identification Credential program by mid-2007. More specifically, it required DHS to implement Transportation Worker Identification Credential at the 10 highest risk ports by July 1, 2007; conduct a pilot program to test various aspects relating to Transportation Worker Identification Credential security card readers including access control technologies in the maritime environment; issue regulations requiring Transportation Worker Identification Credential card readers based on the findings of the pilot; and periodically report to Congress on the status of the program. DHS is taking steps to address these requirements, such as establishing a rollout schedule for enrolling workers and issuing Transportation Worker Identification Credential cards at ports and conducting a pilot program to test Transportation Worker Identification Credential access control technologies. However, we identified a number of challenges. For example, while DHS reports taking steps to address contract planning and oversight problems, the effectiveness of these steps will not be clear until implementation of the Transportation Worker Identification Credential program begins. Additionally, significant challenges remain in enrolling about 770,000 persons at about 3,500 facilities in the Transportation Worker Identification Credential program. Sufficient communication and coordination to ensure that all individuals and organizations affected by the Transportation Worker Identification Credential program are aware of their responsibilities will require concerted effort on the part of DHS and the enrollment contractor. Further DHS and industry stakeholders need to address challenges regarding Transportation Worker Identification Credential access control technologies to ensure that the program is implemented effectively. Without fully testing all aspects of the technology, DHS may not be able ensure that the Transportation Worker Identification Credential access control technology can meet the requirements of the system. For more information, see GAO-07-754T; *Transportation Security: TSA Has Made Progress in Implementing the Transportation Worker Identification Credential Program, but Challenges Remain,* GAO-07-681T; *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program,* GAO-06-982; *Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges,* GAO-05-448T; and *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program,* GAO-05-106. Also, see Department of Homeland Security Office of Inspector General, *DHS Must Address Significant Security Vulnerabilities Prior to TWIC Implementation (Redacted),* OIG-06-47 (Washington, D.C.: July 2006). | |
| | *DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to implement a national facility access control system for port secured areas. DHS reported that the Coast Guard is moving forward with TSA and its contractor to begin enrollments in the Transportation Worker Identification Credential program. DHS stated that Version 1 of the Transportation Worker Identification Credential will contain all of the required biometric information and that a second Notice of Proposed Rulemaking will be published in February 2008 to address the technical requirements for readers that will be used at facilities and aboard vessels. DHS stated that in the meantime, a field test of card reader technology is scheduled for the Long Beach/Los Angeles port complex beginning in July 2007 and that this activity is in compliance with the timeline established in the SAFE Port Act. Further, DHS stated that the Coast Guard will request legislation requiring all persons who are deemed to need unescorted access | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | to the secure areas of regulated vessels and facilities possess a valid Transportation Worker Identification Credential. DHS also reported that the Coast Guard is consolidating a number of merchant mariner licenses and documents into a single Merchant Mariner Credential. This consolidation is described in a supplemental notice of proposed rulemaking that was published in the Federal Register simultaneously with the Transportation Worker Identification Credential final rule on January 25, 2007, which will result in an effective date of March 26, 2007.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although DHS has taken some actions to implement a national facility access control system for port secured areas, more work is needed for the department to achieve this performance expectation. As our previous work demonstrated, DHS faces a number of problems in implementing the Transportation Worker Identification Credential, such as ensuring that access control technology meets system requirements and ensuring sufficient communication and coordination so that all individuals and organizations affected by the Transportation Worker Identification Credential program are aware of their responsibilities. Further, while DHS reported a number of actions it has taken to meet this expectation, it did not provide us with documentation for some aspects of its efforts. For example, DHS did not provide us with documentation showing that it is making progress in starting enrollments. | |
| 11. Implement a port security grant program to help facilities improve their security capabilities | *GAO and DHS IG findings and our assessment:* We conclude that DHS has generally achieved this performance expectation. The port security grant program provides assistance to nonfederal stakeholders for making security improvements at the nation's ports. During fiscal years 2002 through 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. For fiscal year 2006 the DHS appropriations act provided $175 million for the port security grant program, and in fiscal year 2007 the appropriations act provided $210 million for the program. While DHS has made progress in applying risk management to the port security grant program, it faces challenges in strengthening its approach, as demonstrated in part by its experience in awarding past grants. For example, DHS 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. In February 2006 the DHS IG reported that DHS had improved the administration and effectiveness of the most recent round of port security grants, which totaled $142 million for 132 projects. For example, the DHS IG reported that DHS had directed funds to the nation's 66 highest risk ports using a risk-based formula and tiering process and had instituted a new funding allocation model. However, the DHS IG also found several challenges, identifying, for example, 20 projects that reviewers determined did not meet national security priorities but were funded nonetheless. In its fiscal year 2006 Performance and Accountability Report, DHS reported that a risk-based grant allocation process was completed in the third quarter of fiscal year 2006 and was a critical component of the process by which allocations were determined for the Port Security Grant Program. For more information, see *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure,* GAO-06-91. Also, see Department of Homeland Security Office of Inspector General, *Follow Up Review of the Port Security Grant Program,* OIG-06-24 (Washington, D.C.: February 2006, Revised) and Department of Homeland Security Office of Inspector General, *Review of the Port Security Grant Program,* OIG-05-10 (Washington, D.C.: January 2005). | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 12. Develop a national plan to establish and improve maritime intelligence | *GAO findings:* We generally have not conducted work on DHS's efforts to develop a national plan to establish and improve maritime intelligence, and as a result we cannot make an assessment of the extent to which DHS has taken actions to address this performance expectation.<br>*DHS updated information:* In March and May 2007, DHS provided us with updated information on its efforts to develop a national plan to establish and improve maritime intelligence. DHS reported that the President approved the Global Maritime Intelligence Integration Plan in October 2005 in support of the National Strategy for Maritime Security.<br>*Our assessment:* We did not make an assessment of DHS's progress in achieving this performance expectation. While DHS reported that the President approved the Global Maritime Intelligence Integration Plan, we were not able to determine the extent to which the plan has established and improved maritime intelligence. | No assessment made |
| 13. Establish operational centers to monitor threats and fuse intelligence and operations at the regional/port level | *GAO findings:* DHS has established operational centers to monitor threats and fuse intelligence and operations at the regional/port level. In April 2005, we reported that the Coast Guard had two Maritime Intelligence Fusion Centers, located on each coast, that receive intelligence from, and provide intelligence to, the Coast Guard Intelligence Coordination Center. Maritime Intelligence Fusion Centers also provide actionable intelligence to Coast Guard commanders at the district and port levels and share that analysis with interagency partners. Another approach at improving information sharing and port security operations involves interagency operational centers—command centers that bring together the intelligence and operational efforts of various federal and nonfederal participants. In April 2007, we reported that three ports currently have such centers, which are designed to have a unified command structure that can act on a variety of incidents ranging from possible terrorist attacks to search and rescue and environmental response operations. Several new interagency operational centers are about to come on line, but in continuing the expansion, DHS may face such challenges as creating effective working relationships and dealing with potential coordination problems. We also reported that the Coast Guard has the authority to create area committees—composed of federal, state, local, and industry members—that help to develop the area plan for the port. Area committees serve as forums for port stakeholders, facilitating the dissemination of information through regularly scheduled meetings, issuance of electronic bulletins, and sharing key documents. As of June 2006, the Coast Guard had organized 46 area committees. Each has flexibility to assemble and operate in a way that reflects the needs of its port area, resulting in variations in the number of participants, the types of state and local organizations involved, and the way in which information is shared. The Coast Guard also reported that it had implemented a maritime monitoring system—known as the Common Operating Picture system—that fuses data from different sources. According to the Coast Guard, this system is the primary tool for Coast Guard commanders in the field to attain maritime domain awareness. For more information, see GAO-07-754T; *Maritime Security: Information sharing Efforts Are Improving,* GAO-06-933T; *Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention,* GAO-05-394; and GAO-05-448T.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to establish operational centers to monitor threats and fuse intelligence and operations at the regional/port level. DHS reported that at the port level, it is using pre-existing, primarily Coast Guard, command centers to foster information sharing and coordination of the operations of various federal and nonfederal participants. However, DHS noted that in most locations, these efforts are hampered by the limitations of pre-9/11 technology and physical space constraints. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | *Our assessment:* We conclude that DHS has generally achieved this performance expectation. The Coast Guard established two regional Maritime Intelligence Fusion Centers, one on each coast. Further, the Coast Guard, with local federal port security stakeholders, has established three interagency operational centers with several new centers scheduled to come on line, and as of June 2006, the Coast Guard had organized 46 area committees. | |
| 14. Collect information on incoming ships to assess risks and threats | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has taken steps to collect information on incoming ships to assess risks and threats. This includes information relating to, for example, crew, passengers, and cargo. In March 2004, we reported that the Coast Guard had extended the former 24-hour notice of arrival prior to entering a United States port to 96 hours. The information provided with the notice of arrival includes details on the crew, passengers, cargo, and the vessel itself. This increase in notice has enabled the Coast Guard to screen more vessels in advance of arrival and allows additional time to prepare for boardings. For more information, see *Coast Guard Programs: Relationship between Resources Used and Results Achieved Needs to Be Clearer,* GAO-04-432. | Generally achieved |
| 15. Develop a vessel-tracking system to improve intelligence and maritime domain awareness on vessels in U.S. waters | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has made progress in developing a vessel-tracking system to improve intelligence/maritime domain awareness on vessels in U.S. waters. The Nationwide Automatic Identification System uses a device aboard a vessel to transmit an identifying signal to a receiver located at the seaport and other ships in the area. This signal gives seaport officials and other vessels nearly instantaneous information and awareness about a vessel's identity, position, speed, and course. The Coast Guard intends to provide Nationwide Automatic Identification System coverage to meet maritime domain awareness requirements in all navigable waters of the United States and farther offshore. As of May 2005, the Coast Guard had Nationwide Automatic Identification System coverage in several seaports and coastal areas. For more information, see GAO-05-448T and *Maritime Security: Partnering Could Reduce Federal Costs and Facilitate Implementation of Automatic Vessel Identification System,* GAO-04-868. | Generally achieved |
| 16. Develop a long-range vessel-tracking system to improve maritime domain awareness | *GAO findings:* While DHS has taken steps to develop a long-range vessel-tracking system, more work remains. In May 2005 we testified that the Coast Guard was working with the International Maritime Organization to develop functional and technical requirements for long-range tracking out to 2,000 nautical miles and had proposed an amendment to the International Convention for Safety of Life at Sea for this initiative. The International Maritime Organization adopted amendments for the long-range identification and tracking of ships in May 2006. We have also reported that a recently passed International Maritime Organization requirement calls for most commercial vessels, including tankers, to begin transmitting identification and location information on or before December 31, 2008, to Safety of Life at Sea contracting governments under certain specified circumstances. This will allow the vessels to be tracked over the course of their voyages. Under this requirement, information on the ship's identity, location, date, and time of the position will be made available to the ship's flag state, the ship's destination port state, and any coastal state within 1,000 miles of the ship's route. For more information, see GAO-05-448T.<br>*DHS updated information:* In March, April, and June 2007, DHS provided us with updated information on its efforts to develop a long-range vessel-tracking system to improve maritime domain awareness. DHS reported that it has classified and unclassified means available to perform long-range tracking. DHS stated that unclassified systems, including the Nationwide Automatic Identification System, are currently in the process of being fielded. DHS reported that the Nationwide Automatic | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | Identification System, when implemented, will provide automatic identification system coverage from commercial satellites in all U.S. waters and up to 2,000 miles offshore. DHS stated that it expects initial capability in 2007. DHS also stated that it purchases tracking data from commercial sources in places where those capabilities are not currently fielded by the United States Coast Guard. DHS reported that work is in progress to establish a system through the International Maritime Organization that will provide an unclassified global tracking capability by 2008 as a part of an existing International Maritime Organization convention and give the United States a system that is compatible and interoperable with the Global maritime community. DHS reported that the Coast Guard will need to establish the capability to receive signals and interact with the International Maritime Organization's international data center and that the Coast Guard has funded various studies and demonstrations to address the implementation of long-range-tracking. Further, DHS reported that the Coast Guard has developed rule-making language that supports the International Maritime Organization rules regarding implementation of long-range tracking under the recently approved Safety of Life at Sea Chapter V. DHS stated that the proposed rule-making is in final development and is expected to be published for comment later this year.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has some vessel-tracking capabilities and is working with the International Maritime Organization to develop a long-range vessel-tracking system. However, DHS did not provide evidence that it has developed a long-range vessel-tracking system out to 2,000 nautical miles. | |
| 17. Collect information on arriving cargo for screening purposes | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. DHS collects information on arriving cargo for screening purposes.[a] Pursuant to federal law, CBP required ocean carriers to electronically transmit cargo manifests to CBP's Automated Manifest System 24 hours before the cargo is loaded on a ship at a foreign port. In March 2004 we reported that according to CBP officials we contacted, although no formal evaluations had been done, the 24-hour rule was beginning to improve both the quality and timeliness of manifest information. CBP officials acknowledged, however, that although improved, manifest information had not always provided accurate or reliable data for targeting purposes. For more information see *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts,* GAO-05-557 and 04-577T. | Generally achieved |
| 18. Develop a system for screening and inspecting cargo for illegal contraband | *GAO and DHS IG findings and our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed a system for screening incoming cargo for illegal contraband—called the Automated Targeting System.[b] However, our previous work has identified a number of challenges to the implementation of this program. CBP employs its Automated Targeting System computer model to review documentation on all arriving containers and help select or target containers for additional scrutiny. The Automated Targeting System was originally designed to help identify illegal narcotics in cargo containers, but was modified to help detect all types of illegal contraband used by smugglers or terrorists. In addition, CBP has a program, called the Supply Chain Stratified Examination, which supplements the Automated Targeting System by randomly selecting additional containers to be physically examined. We identified a number of challenges to the implementation of the Automated Targeting System. For example, in March 2006 we testified that CBP did not yet have key controls in place to provide reasonable assurance that the Automated Targeting System was effective at targeting oceangoing cargo containers with the highest risk of containing smuggled weapons of mass destruction. Further, we reported that while CBP strove to refine the Automated Targeting System to include intelligence information it acquires and feedback it receives from its targeting officers at the seaports, it was not able to | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | systematically adjust the system for inspection results. In November 2006, the DHS IG reported that national Automatic Targeting System performance measures were still being developed to determine the effectiveness of the Automatic Targeting System oceangoing container targeting system. The DHS IG also found that that CBP did not use all intelligence/information sources available for targeting purposes. In April 2007 we reported CBP faced the challenge of implementing the program while internal controls are being developed. CBP's vital mission does not allow it to halt its screening efforts while it puts these controls in place, and CBP thus faces the challenge of ensuring that it inspects the highest-risk containers even though it lacks information to optimally allocate inspection resources. For more information, see GAO-07-754T; *Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System,* GAO-06-591T; and *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection,* GAO-04-557T. Also, see Department of Homeland Security Office of Inspector General, *Audit of Targeting Oceangoing Cargo Containers (Unclassified Summary),* OIG-07-09 (Washington, D.C.: November 2006) and Department of Homeland Security Office of Inspector General, *Audit of Targeting Oceangoing Cargo Containers (Unclassified Summary),* OIG-05-26 (Washington, D.C.: July 2005). | |
| 19. Develop a program to screen incoming cargo for radiation | *GAO findings:* While DHS has taken steps to develop a program to screen incoming cargo for radiation, challenges remain.[c] As of December 2005, DHS had deployed 670 of 3,034 radiation portal monitors—about 22 percent of the portal monitors DHS plans to deploy. As of February 2006, CBP estimated that with these deployments CBP had the ability to screen about 62 percent of all containerized shipments entering the United States, and roughly 77 percent of all private vehicles. Within these total percentages, CBP could screen 32 percent of all containerized seaborne shipments; 90 percent of commercial trucks and 80 percent of private vehicles entering from Canada; and approximately 88 percent of all commercial trucks and 74 percent of all private vehicles entering from Mexico. However, in March 2006 we reported that the deployment of portal monitors had fallen behind schedule, making DHS's goal of deploying 3,034 by 2009 unlikely. Further, in October 2006 we reviewed DHS's cost-benefit analysis for the deployment and purchase of $1.2 billion worth of new portal monitors. We found that DHS's cost-benefit analysis did not provide a sound analytical basis for the decision to purchase and deploy new portal monitor technology. For example, DHS did not use the results of its own performance tests in its cost-benefit analysis and instead relied on assumptions of the new technology's anticipated performance level. Further, the department's analysis did not include all of the major costs and benefits required by DHS guidelines. Finally, DHS used questionable assumptions in estimating the costs of current portal monitors. In March 2007 we reported that DHS has not yet collected a comprehensive inventory of testing information on commercially available polyvinyl toluene portal monitors. Such information—if collected and used—could improve the Domestic Nuclear Detection Office's understanding of how well portal monitors detect different radiological and nuclear materials under varying conditions. In turn, this understanding would assist the Domestic Nuclear Detection Office's future testing, development, deployment, and purchases of portal monitors. Further, while DHS is improving its efforts to provide technical and operational information about radiation portal monitors to state and local authorities, some state representatives with whom we spoke, particularly those from states with less experience conducting radiation detection programs, would like to see the Domestic Nuclear Detection Office provide more prescriptive advice on what types of radiation detection equipment to deploy and how to use it. For more information, see *Combating Nuclear Smuggling: DHS's Decision to Procure and Deploy the Next Generation of Radiation Detection Equipment Is Not Supported by Its Cost-Benefit Analysis,* GAO-07-581T;*Combating Nuclear Smuggling: DNDO Has Not Yet Collected Most of the National Laboratories' Test Results on* | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | *Radiation Portal Monitors in Support of DNDO's Testing and Development Program,* GAO-07-347R; *Combating Nuclear Smuggling: DHS's Cost-Benefit Analysis to Support the Purchase of New Radiation Detection Portal Monitors Was Not Based on Available Performance Data and Did Not Fully Evaluate All the Monitors' Costs and Benefits,* GAO-07-133R; and *Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports-of-Entry, but Concerns Remain,* GAO-06-389.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to develop a program to screen incoming cargo for radiation. DHS reported that the Coast Guard continues to develop the procedures and capabilities for detecting chemical, biological, radiological, nuclear and high-yield explosive threats in the maritime environment. DHS reported that through these efforts, the Coast Guard has partnered with the Domestic Nuclear Detection Office and reported that it partnered with the Federal Bureau of Investigation, Department of Energy, and Department of Defense. DHS stated that the Coast Guard maintains three dedicated response teams, on call 365 days a year, to respond to and mitigate various environmental incidents. DHS reported that the Coast Guard has distributed personal radiation detectors, hand-held isotope identifiers, and radiation sensor backpacks to the field, and continues to pursue procurement of additional equipment through a joint acquisition strategy with Domestic Nuclear Detection Office. Further, DHS as of March 9, 2007, CBP had deployed 966 radiation portal monitors. DHS stated that these deployments provide CBP with the capability to screen approximately 91 percent of containerized cargo and 88 percent of personally owned vehicles entering the United States. DHS further stated that within these totals, CBP could screen about 89 percent of seaborne containerized cargo; 91 percent of commercial trucks and about 81 percent of personally owned vehicles arriving from Canada; and 96 percent of commercial trucks and 91 percent of personally owned vehicles arriving from Mexico.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. In our prior work, we reported that DHS was unlikely to reach its 2009 goal for radiation portal deployment. We also reported that in conducting its cost-benefit analysis of the decision to purchase and deploy new portal monitor technology, DHS did not include all of the major costs and benefits required by DHS guidelines and did not use the results of its own performance tests. The department instead relied on assumptions of the new technology's anticipated performance level. The lack of adequate means for acquiring technology is a major impediment to the development and implementation of the program. | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 20. Develop a program to work with foreign governments to inspect suspicious cargo before it leaves for U.S. ports | *GAO findings:* DHS has developed a program to work with foreign governments to inspect suspicious cargo before leaving for U.S. ports. Announced in January 2002, the Container Security Initiative program was implemented to allow CBP officials to target containers at foreign seaports so that any high-risk containers may be inspected prior to their departure for U.S. destinations. The Security and Accountability for Every Port Act, which took effect in October 2006, codified the Container Security Initiative. CBP first solicited the participation of the 20 foreign ports that shipped the highest volume of ocean containers to the United States. These top 20 ports are located in 14 countries and regions and shipped a total of 66 percent of all containers that arrived in U.S. seaports in 2001. CBP has since expanded the Container Security Initiative to strategic ports, which may ship lesser amounts of cargo to the United States but may also have terrorism or geographical concerns. We identified a number of challenges to the Container Security Initiative. For example, in April 2005 we reported that staffing imbalances were impeding CBP from targeting all containers shipped from Container Security Initiative ports before they leave for the United States. However, we reported that CBP had been unable to staff the Container Security Initiative teams at the levels called for in the Container Security Initiative staffing model because of diplomatic and practical considerations. In terms of diplomatic considerations, the host government may limit the overall number of U.S. government employees to be stationed in the country and may restrict the size of the Container Security Initiative team. In terms of practical considerations, the host governments may not have enough workspace available for Container Security Initiative staff and may thus restrict the size of the Container Security Initiative team. The U.S. Department of State would also have to agree to the size of the Container Security Initiative teams, a decision that has to be balanced with the mission priorities of the embassy, the programmatic and administrative costs associated with increases in staffing, and security issues related to the number of Americans posted overseas. We reported that as a result of these staff imbalances, 35 percent of U.S.-bound shipments from Container Security Initiative ports were not targeted and were therefore not subject to inspection overseas. We also reported the existence of limitations in one data source Container Security Initiative teams use for targeting high-risk containers. In April 2007 we reported that the number of seaports that participate in the program had grown to 50, with plans to expand to a total of 58 ports by the end of this fiscal year. We also identified several challenges to the Container Security Initiative. For example, we reported that there are no internationally recognized minimum technical requirements for the detection capability of nonintrusive inspection equipment used to scan containers. Consequently, host nations at Container Security Initiative seaports use various types of nonintrusive inspection equipment, and the detection capabilities of such equipment can vary. Further, we reported that some containers designated as high-risk did not receive an inspection at the Container Security Initiative seaport. Containers designated as high-risk by Container Security Initiative teams that are not inspected overseas (for a variety of reasons) are supposed to be referred for inspection upon arrival at the U.S. destination port. However, CBP officials noted that between July and September 2004, only about 93 percent of shipments referred for domestic inspection were inspected at a U.S. seaport. According to CBP, it is working on improvements in its ability to track such containers to ensure that they are inspected. We have ongoing work to further assess the Container Security Initiative. For more information, see GAO-07-754T; *Homeland Security: Key Cargo Security Programs Can Be Improved,* GAO-05-466T; *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts,* GAO-05-557; *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection,* GAO-04-557T; and *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors,* GAO-03-770. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | *DHS updated information*: In March and April 2007, DHS provided us with updated information on its efforts to develop a program to work with foreign governments to inspect suspicious cargo before it leaves for U.S. ports. DHS reported that in April 2005 the Container Security Initiative began implementing revisions to the Container Security Initiative staffing model to have optimal levels of staff at Container Security Initiative ports to maximize the benefits of targeting and inspection activities, in conjunction with host nation customs officials, and to increase its staff at the National Targeting Center in the United States to complement the work of targeters overseas. DHS stated that this enabled Container Security Initiative ports to review and screen 100 percent of manifest information for containers destined to the United States.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. The department has developed a program to work with foreign governments to inspect suspicious cargo before it leaves for U.S. ports. DHS has developed the Container Security Initiative, and the program allows CBP officials to target containers at foreign seaports for inspection. However, our previous work has identified a number of challenges to the implementation of this program, such as the detection capabilities of host nations' inspection equipment. | |
| 21. Develop a program to work with the private sector to improve and validate supply chain security | *GAO findings:* DHS has developed a program to work with the private sector to improve and validate supply chain security, but some challenges remain. Initiated in November 2001, the Customs-Trade Partnership Against Terrorism is a voluntary program designed to improve the security of the international supply chain while maintaining an efficient flow of goods. Under the Customs-Trade Partnership Against Terrorism, CBP officials work in partnership with private companies to review their supply chain security plans to improve members' overall security. In return for committing to making improvements to the security of their shipments by joining the program, Customs-Trade Partnership Against Terrorism members may receive benefits that result in reduced scrutiny of their shipments. The Security and Accountability For Every Port Act, which took effect in October 2006, codified the program. In April 2007, we reported that since the inception of the Customs-Trade Partnership Against Terrorism, CBP has certified 6,375 companies, and as of March 2007, it had validated the security of 3,950 of them (61.9 percent). We also reported that while CBP initially set a goal of validating all companies within their first 3 years as Customs-Trade Partnership Against Terrorism members, the program's rapid growth in membership made the goal unachievable. CBP then moved to a risk-based approach to selecting members for validation, considering factors such as the company having foreign supply chain operations in a known terrorist area or involving multiple foreign suppliers. CBP further modified its approach to selecting companies for validation to achieve greater efficiency by conducting "blitz" operations to validate foreign elements of multiple members' supply chains in a single trip. Blitz operations focus on factors such as Customs-Trade Partnership Against Terrorism members within a certain industry, supply chains within a certain geographic area, or foreign suppliers to multiple Customs-Trade Partnership Against Terrorism members. Risks remain a consideration, according to CBP, but the blitz strategy drives the decision of when a member company will be validated. However, we identified a number of challenges to Customs-Trade Partnership Against Terrorism. For example, CBP's standard for validations—to ensure that members' security measures are reliable, accurate and effective—is hard to achieve. Since the Customs-Trade Partnership Against Terrorism is a voluntary rather than a mandatory program, there are limits on how intrusive CBP can be in its validations. Further, challenges developing Customs-Trade Partnership Against Terrorism outcome-based performance measures persist because of difficulty measuring deterrent effect. CBP has contracted with the University of Virginia for help in developing useful measures. We have ongoing work to further assess the Customs-Trade Partnership Against Terrorism program. For more | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | information, see GAO-07-754T; *Homeland Security: Key Cargo Security Programs Can Be Improved,* GAO-05-466T; *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security,* GAO-05-404; and *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors,* GAO-03-770.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to develop a program to work with the private sector to improve and validate supply chain security. For example, DHS reported that the Customs-Trade Partnership Against Terrorism program now has a Web based portal system that allows data storage and statistical tracking of all participants and also allows for reports to be run ensuring that performance goals are being met. DHS also stated that the Customs-Trade Partnership Against Terrorism reached its full staffing level of 156 Supply Chain Security Specialists in December of 2006.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. The department has developed a program to work with the private sector to improve and validate supply chain security. Through the Customs-Trade Partnership Against Terrorism, DHS officials work in partnership with private companies to improve members' overall security. However, our previous work has identified a number of challenges to the implementation of this program. For example, because the Customs-Trade Partnership Against Terrorism is a voluntary program, CBP is limited in how intrusive its validations can be, and CBP also faces challenges in developing outcome-based performance measures for the program. | |
| 22. Develop standards for cargo containers to ensure their physical security | *GAO findings and assessment:* We generally have not conducted work on DHS's efforts to develop standards to better secure containers, and as a result we cannot make an assessment of the extent to which DHS has taken actions to address this performance expectation. | No assessment made |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 23. Develop an international port security program to assess security at foreign ports | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed a program to assess security at foreign ports. However, our previous work has identified a number of challenges to the implementation of this program. To help secure the overseas supply chain, the Maritime Transportation Security Act required the Coast Guard to develop a program to assess security measures in foreign ports and, among other things, recommend steps necessary to improve security measures in their ports. In April 2007, we reported that the Coast Guard established this program, called the International Port Security Program, in April 2004. Under this program, the Coast Guard and host nations review the implementation of security measures in the host nations' ports against established security standards, such as the International Maritime Organization's International Ship and Port Facility Security Code. Coast Guard teams have been established to conduct country visits, discuss security measures implemented, and collect and share best practices to help ensure a comprehensive and consistent approach to maritime security in ports worldwide. The conditions of these visits, such as timing and locations, are negotiated between the Coast Guard and the host nation. Coast Guard officials also make annual visits to the countries to obtain additional observations on the implementation of security measures and ensure deficiencies found during the country visits are addressed. As of April 2007, the Coast Guard reported that it has visited 86 countries under this program and plans to complete 29 more visits by the end of fiscal year 2007. We are currently conducting a review of the Coast Guard's international enforcement programs, such as the International Port Security Program. Although this work is still in process and not yet ready to be included in this assessment, we have completed a more narrowly scoped review required under the Security and Accountability For Every Port Act regarding security at ports in the Caribbean Basin. As part of this work, we looked at the efforts made by the Coast Guard in the region under the program and the Coast Guard's findings from the country visits it made in the region. In this review we found a number of challenges concerning program implementation. For example, for the countries in this region for which the Coast Guard had issued a final report, the Coast Guard reported that most had "substantially implemented the security code," while one country that was just recently visited was found to have not yet implemented the code and will be subject to a reassessment. At the facility level, the Coast Guard found several facilities needing improvements in areas such as access controls, communication devices, fencing, and lighting. Because our review of the Coast Guard's International Port Security Program is still ongoing, we have not yet reviewed the results of the Coast Guard's findings in other regions of the world. While our larger review is still not complete, Coast Guard officials have told us they face challenges in carrying out this program in the Caribbean Basin. These challenges include ensuring sufficient numbers of adequately trained personnel and addressing host nation sovereignty issues. For more information, see GAO-07-754T and GAO-05-448T. | Generally achieved |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

[a]The terms “inspecting” and “screening” have been used interchangeably to denote some level of examination of a person or good, which can entail a number of different actions, including manual physical inspections to ensure that cargo does not contain weapons, explosives, or stowaways, or inspections using noninstrusive technologies that do not require the cargo to be opened in order to be inspected. However, for this performance expectation, we use the term “inspect” to refer to this broad range of activities and “screening” to refer to an assessment of the security risk posed by a container based on available information.

[b]The terms “inspecting” and “screening” have been used interchangeably to denote some level of examination of a person or good, which can entail a number of different actions, including manual physical inspections to ensure that cargo does not contain weapons, explosives, or stowaways, or inspections using noninstrusive technologies that do not require the cargo to be opened in order to be inspected. However, for this performance expectation, we use the term “inspect” to refer to this broad range of activities and “screening” to refer to an assessment of the security risk posed by a container based on available information.

[c]The terms “inspecting” and “screening” have been used interchangeably to denote some level of examination of a person or good, which can entail a number of different actions, including manual physical inspections to ensure that cargo does not contain weapons, explosives, or stowaways, or inspections using noninstrusive technologies that do not require the cargo to be opened in order to be inspected. For this performance expectation, we use the terms “screen” and “inspect” to refer to this broad range of activities.

## DHS Has Made Limited Progress in Its Emergency Preparedness and Response Efforts

Several federal legislative and executive provisions support preparation for and response to emergency situations. The Robert T. Stafford Disaster Relief and Emergency Assistance Act (the Stafford Act)[25] primarily establishes the programs and processes for the federal government to provide major disaster and emergency assistance to state, local, and tribal governments; individuals; and qualified private nonprofit organizations. FEMA, within DHS, has responsibility for administering the provisions of the Stafford Act. FEMA’s emergency preparedness and response efforts include programs that prepare to minimize the damage and recover from terrorist attacks and disasters; help to plan, equip, train, and practice needed skills of first responders; and consolidate federal response plans and activities to build a national, coordinated system for incident management. DHS’s emergency preparedness and response efforts have been affected by DHS reorganizations and, in the wake of the 2005 Gulf Coast hurricanes, reassessments of some initiatives, such as the National Response Plan and its Catastrophic Incident Supplement. DHS is undergoing its second reorganization of its emergency preparedness and response programs in about 18 months. The first reorganization was initiated by the Secretary of Homeland Security in the summer of 2005 and created separate organizations within DHS responsible for preparedness and for response and recovery. The second reorganization was required by

[25]The Stafford Act is codified as amended at 42 U.S.C. § 5121 et seq.

the fiscal year 2007 DHS appropriations act and largely took effect on April 1, 2007.

As shown in table 28, we identified 24 performance expectations for DHS in the area of emergency preparedness and response and found that overall DHS has made limited progress in meeting those performance expectations. In particular, we found that DHS has generally achieved 5 performance expectations and has generally not achieved 18 others. For 1 performance expectation, we did not make an assessment.

Table 28: Performance Expectations and Progress Made in Emergency Preparedness and Response

| | Assessment | | |
|---|---|---|---|
| Performance expectation | Generally achieved | Generally not achieved | No assessment made |
| 1. Establish a comprehensive training program for national preparedness | | ✓ | |
| 2. Establish a program for conducting emergency preparedness exercises | ✓ | | |
| 3. Conduct and support risk assessments and risk management capabilities for emergency preparedness | | ✓ | |
| 4. Ensure the capacity and readiness of disaster response teams | | ✓ | |
| 5. Develop a national incident management system | ✓ | | |
| 6. Coordinate implementation of a national incident management system | | ✓ | |
| 7. Establish a single, all-hazards national response plan | | ✓ | |
| 8. Coordinate implementation of a single, all-hazards response plan | | ✓ | |
| 9. Develop a complete inventory of federal response capabilities | | ✓ | |
| 10. Develop a national, all-hazards preparedness goal | | ✓ | |
| 11. Support citizen participation in national preparedness efforts | | | ✓ |
| 12. Develop plans and capabilities to strengthen nationwide recovery efforts | | ✓ | |
| 13. Develop the capacity to provide needed emergency assistance and services in a timely manner | | ✓ | |
| 14. Provide timely assistance and services to individuals and communities in response to emergency events | | ✓ | |
| 15. Implement a program to improve interoperable communications among federal, state, and local agencies | | ✓ | |
| 16. Implement procedures and capabilities for effective interoperable communications | | ✓ | |

| Performance expectation | Assessment |  |  |
|---|---|---|---|
|  | Generally achieved | Generally not achieved | No assessment made |
| 17. Increase the development and adoption of interoperability communications standards |  | ✓ |  |
| 18. Develop performance goals and measures to assess progress in developing interoperability |  | ✓ |  |
| 19. Provide grant funding to first responders in developing and implementing interoperable communications capabilities | ✓ |  |  |
| 20. Provide guidance and technical assistance to first responders in developing and implementing interoperable communications capabilities |  | ✓ |  |
| 21. Provide assistance to state and local governments to develop all-hazards plans and capabilities |  | ✓ |  |
| 22. Administer a program for providing grants and assistance to state and local governments and first responders | ✓ |  |  |
| 23. Allocate grants based on assessment factors that account for population, critical infrastructure, and other risk factors | ✓ |  |  |
| 24. Develop a system for collecting and disseminating lessons learned and best practices to emergency responders |  | ✓ |  |
| **Total** | **5** | **18** | **1** |

Source: GAO analysis.

Note: An assessment of “generally achieved” indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of “generally achieved” does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, “generally not achieved” indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of “generally not achieved” may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated “no assessment made.”

Table 29 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of emergency preparedness and response and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation’s key elements (generally not achieved).

**Table 29: Performance Expectations and Assessment of DHS Progress in Emergency Preparedness and Response**

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Establish a comprehensive training program for national preparedness | *GAO and DHS IG findings:* DHS has developed and implemented various training programs, but it is unclear how these programs contribute or link to a comprehensive training program for national preparedness. In July 2005, we reported that according to DHS's National Training and Exercises and Lessons Learned Implementation Plan, DHS intended to implement a system to develop and maintain state and local responders' all-hazards capabilities. The goal of this system was to provide integrated national programs for training, exercise, and lessons learned that would reorient existing initiatives at all government levels in order to develop, achieve, and sustain the capabilities required to achieve the National Preparedness Goal. As part of this system, DHS intended to implement a national training program including providing criteria for accreditation of training courses, a national directory of accredited training providers, and a National Minimum Qualification Standards Guide. In March 2006, the DHS IG reported that FEMA provided regular training for emergency responders at the federal, state, and local levels; managed the training and development of FEMA employees internally; and provided disaster-specific training through the Disaster Field Training Operations cadre. FEMA's Training Division increased the size and number of classes it delivered, even as budgets decreased. The DHS IG found that courses provided by the Emergency Management Institute were one of FEMA's primary interactions with state and local emergency managers and responders. However, the DHS IG reported that the ability of Emergency Management Institute classes to improve emergency management during a hurricane was not quantifiable with available measurements. The DHS IG reported that employee development lacked the resources and organizational alignment to improve performance. Specifically, the DHS IG reported that FEMA had no centralized and comprehensive information on employee training. FEMA used several incompatible systems, including databases operated by the Employee Development branch, Emergency Management Institute, Disaster Field Training Operations cadre, and information technology security. Additional classes, including classes provided at conferences, classes provided by state or local entities, and leadership training courses, were not consistently tracked. The DHS IG reported that FEMA regional training managers maintained records on their own, drawing from each of these systems. The DHS IG concluded that not only was this process inefficient and susceptible to error, it also complicated efforts to monitor employee development of mission-critical skills and competencies. For more information, see *Statement by Comptroller General David M. Walker on GAO's Preliminary Observations Regarding Preparedness and Response to Hurricanes Katrina and Rita,* GAO-06-365R and *Homeland Security: DHS's Efforts to Enhance First Responders' All-Hazards Capabilities Continue to Evolve,* GAO-05-652. Also, see Department of Homeland Security Office of Inspector General, *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina,* OIG-06-32 (Washington, D.C.: March 2006).<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to establish a comprehensive training program for national preparedness. DHS has developed a series of training programs on the National Response Plan and the National Incident Management System to improve national preparedness. In particular, DHS reported that more than 100 Office of Grants and Training-supported courses are available to emergency responders and that in fiscal year 2006, there were more than 336,000 participants in Office of Grants and Training courses. DHS has also developed and implemented a Multi-Year Training and Exercise Plan designed to guide states in linking training and exercise activities. According to DHS, states identify priorities in their state strategies, translate them into target capabilities that they need to build, and then attend a workshop in which they build a schedule for training and exercises to address the capabilities. DHS reported that course content in the National Training Program is being aligned to target capabilities so that there is a direct link between the capabilities a state needs to build and the courses that its responders need to take to build those skills. In addition, DHS reported that the U.S. Fire Administration's National Fire Academy and | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | FEMA's Emergency Management Institute have coordinated to develop a curriculum for first responder training across federal, state, local, and tribal governments and that in fiscal year 2006, more than 26,000 and 13,000 students attended training at the National Fire Academy and the Emergency Management Institute, respectively. DHS noted that with the re-creation of the National Integration Center in FEMA's new National Preparedness Directorate, FEMA will be coordinating development of a comprehensive national training strategy to ensure course curriculum is consistent among training facilities and to avoid duplication or overlap.<br>*Our assessment:* Until DHS issues a comprehensive national training strategy, we conclude that DHS has generally not achieved this performance expectation. Although DHS has developed and implemented a variety of training programs related to national preparedness, specifically on the National Response Plan and National Incident Management System, DHS did not provide us with evidence on how these various programs have contributed to the establishment of a comprehensive, national training program. Moreover, DHS reported that it is working to develop a comprehensive national training strategy, but did not provide us with a target time frame for completing and issuing the national strategy. | |
| 2. Establish a program for conducting emergency preparedness exercises | *GAO and DHS IG findings:* DHS has taken actions to establish a program for conducting emergency preparedness exercises, but much more work remains. In July 2005 we reported that as part of its plan for national training, exercises, and lessons learned, DHS intended to establish a national exercise program. This program was intended to reorient the existing National Exercise Program to incorporate the capabilities-based planning process and provide standardized guidance and methodologies to schedule, design, develop, execute, and evaluate exercises at all levels of government. This program was also intended to provide requirements for the number and type of exercises that communities of varying sizes should conduct to meet the National Preparedness Goal. In March 2006, the DHS IG reported on the long-term deterioration in FEMA's exercise program. The DHS IG reported that emergency management exercises were developed to test and validate existing programs, policies, plans, and procedures to address a wide range of disasters to which FEMA must respond. There were numerous types of exercises, ranging from tabletop exercises, where participants discussed actions and responses, to command post exercises, where specific aspects of a situation were exercised, to large-scale exercises, which involved multiple entities and a significant planned event with activation of personnel and resources. Further, the DHS IG reported that FEMA no longer had a significant role in the development, scope, and conduct of state exercises, though FEMA personnel maintained a presence at state events. FEMA participated in exercises administered by other agencies, but those exercises limited FEMA's ability to choose which plans, objectives, and relationships to test. For more information, see GAO-06-365R and GAO-05-652. Also, see Department of Homeland Security Office of Inspector General, *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina,* OIG-06-32 (Washington, D.C.: March 2006).<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to establish a program for conducting emergency preparedness exercises. DHS has developed a Homeland Security Exercise Evaluation Program that, according to DHS, has been adopted by every major federal agency involved in emergency preparedness. This program provides a standardized methodology for exercise design, development, conduct, evaluation, and improvement planning and provides guidance and doctrine for exercises that are conducted with homeland security grant funding. According to DHS, all exercise grant recipients are mandated to comply with Homeland Security Exercise Evaluation Program guidelines. DHS reported that for exercises for which the department collected and analyzed information in fiscal year 2006, 33 out of 48 Direct Support Exercises were compliant with the Homeland Security Exercise Evaluation Program and 40 out of 110 state or locally funded grant exercises were compliant. DHS noted that it has not evaluated regional and national exercises' compliance with the Homeland Security Exercise Evaluation Program. DHS has also developed a Homeland Security Exercise Evaluation Program Toolkit, which is an online system that walks users | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | through scheduling, planning, evaluating, and tracking corrective actions from an exercise. DHS has also developed the Corrective Action Program to track and monitor corrective actions following exercises and the National Exercise Schedule to facilitate the scheduling and synchronization of national, federal, state, and local exercises. In addition, DHS reported that the National Exercise Program charter was approved by the Homeland Security Council, and DHS reported that the National Exercise Program Implementation Plan has been approved by the President and is scheduled to be released shortly.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. The National Exercise Program charter has been established and approved. Moreover, DHS has developed and begun to implement the Homeland Security Exercise Evaluation Program. This program provides standardized guidance and methodologies for scheduling, developing, executing, and evaluating emergency preparedness exercises. | |
| 3. Conduct and support risk assessments and risk management capabilities for emergency preparedness | *GAO findings:* DHS has taken actions to support efforts to conduct risk assessments and develop risk management capabilities for emergency preparedness, but much more work remains. In July 2005 we reported that, according to DHS's Assessment and Reporting Implementation Plan, DHS intended to implement an assessment and reporting system to collect preparedness data to inform decision makers at all levels on the capabilities of the federal government, states, local jurisdictions, and the private sector. According to the plan, DHS intended to collect data from all governmental recipients of direct funding, using states to collect data from local jurisdictions and using federal regulatory agencies and other appropriate sources to collect private sector data. According to DHS, aggregating these data at all levels would provide information needed to allocate resources, execute training and exercises, and develop an annual status report on the nation's preparedness. The purpose of the assessment and reporting system was to provide information about the baseline status of national preparedness and to serve as the third stage of DHS's capability-based planning approach to ensure that state and local first responder capabilities fully support the National Preparedness Goal. For more information, see *Homeland Security: Applying Risk Management Principles to Guide Federal Investments*, GAO-07-386T and GAO-05-652.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to conduct and support risk assessments and risk management capabilities for emergency preparedness. In particular, in April 2007, DHS established the new Office of Risk Management and Analysis to serve as the DHS Executive Agent for national-level risk management analysis standards and metrics; develop a standardized approach to risk; develop an approach to risk management to help DHS leverage and integrate risk expertise across components and external stakeholders; assess DHS risk performance to ensure programs are measurably reducing risk; and communicate DHS risk management in a manner that reinforces the risk-based approach.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS did not provide us with documentation on its efforts to actually conduct risk assessments and support risk management capabilities specifically for emergency preparedness. Moreover, DHS has only recently established the new Office of Risk Management and Analysis, and this office's effect on DHS's efforts to support risk management capabilities for emergency preparedness is not yet known. | Generally not achieved |
| 4. Ensure the capacity and readiness of disaster response teams | *GAO and DHS IG findings:* DHS has faced challenges in ensuring the capacity and readiness of emergency response teams. In our work reviewing the response to Hurricane Katrina, we reported that while there were aspects that worked well, it appeared that logistics systems for critical resources were often totally overwhelmed by the hurricane, with critical resources apparently not available, properly distributed, or provided in a timely manner. We also reported that the magnitude of the affected population in a major catastrophe calls for greater capabilities for disaster response. In March 2006, the DHS IG reported that, historically, FEMA has established a 72-hour time period as the maximum amount of time for emergency response | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | teams to arrive on scene. However, the DHS IG concluded that it was unclear whether this was responsive to the needs of a state and the needs of disaster victims. The DHS IG reported that a 72-hour response time did not meet public expectations, as was vividly demonstrated by media accounts within 24 hours after landfall of Hurricane Katrina. The DHS IG noted that shorter time periods, such as 60 hours, 48 hours, or even 12 hours, had been mentioned. However, to meet this level of expectation, several factors had to be addressed. According to the DHS IG, once strategic performance measures and realistic expectations were established, other actions could be taken to support those response goals. For more information, see GAO-06-365R. Also, see Department of Homeland Security Office of Inspector General, *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina,* OIG-06-32 (Washington, D.C.: March 2006).<br>*DHS updated information:* In March and May 2007, DHS provided us with updated information on its efforts to ensure the capacity and readiness of disaster response teams. DHS reported that FEMA has completed efforts to identify and categorize more than 100 resources, including teams and pieces of equipment, which are then grouped into eight disciplines, such as law enforcement resources, emergency medical services, and search and rescue resources. DHS also provided information on its various disaster response teams currently in use. DHS's Emergency Response Teams-National are to be deployed in response to incidents of national significance and major disasters to coordinate disaster response activities, coordinate and deploy key national response assets and resources, provide situational awareness, and maintain connectivity with DHS operations centers and components. DHS's Emergency Response Teams-Advanced are designed to be deployed in the early phases of an incident to work directly with states to assess disaster impact, gain situational awareness, help coordinate disaster response, and respond to specific state requests for assistance. DHS's Rapid Needs Assessment Teams are small regional teams that are designed to collect disaster information to determine more specific disaster response requirements. In addition, Federal Incident Response Support Teams are designed to serve as the forward component of Emergency Response Teams-Advanced to provide preliminary on-scene federal management in support of the local Incident or Area Commander. DHS has established readiness indicators for the Federal Incident Response Support Teams and Urban Search and Rescue teams have their own indicators, but FEMA officials stated that they have not yet developed readiness indicators for other types of response teams. DHS reported that its Federal Incident Response Teams were tested during Tropical Storm Ernesto and other events, such as tornadoes. In addition, FEMA reported that it is developing a concept for new rapidly deployable interagency incident management teams designed to provide a forward federal presence to facilitate managing the national response for catastrophic incidents, called National Incident Management and Regional Incident Management Teams.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although DHS provided us with documentation on its various response teams and efforts taken to strengthen teams' readiness and capacity, DHS did not provide us with concrete evidence to demonstrate that response teams' readiness and capacity have improved since Hurricanes Katrina and Rita. Although DHS has tested its response team capabilities in several small-scale disasters, they have not been tested in a large-scale disaster. In addition, DHS did not provide us with documentation of the results of exercises, tests, or after-action reports on the small-scale disasters in which the response teams have been used that would indicate enhancements in teams' readiness and capacity. Moreover, DHS has not yet developed readiness indicators for its disaster responses teams other than Urban Search and Rescue and Federal Incident Response Support Teams. | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 5. Develop a national incident management system | *GAO findings:* DHS has developed a national incident management system. The National Incident Management System is a policy document that defines roles and responsibilities of federal, state, and local first responders during emergency events. The intent of the system described in the document is to establish a core set of concepts, principles, terminology, and organizational processes to enable effective, efficient, and collaborative emergency event management at all levels. These concepts, principles, and processes are designed to improve the ability of different jurisdictions and first responder disciplines to work together in various areas—command, resource management, training, and communications. For more information, see *Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System,* GAO-06-618 and GAO-05-652.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on efforts to further develop the National Incident Management System. DHS reported that the National Incident Management System has been undergoing review and revision by federal, state, and local government officials; tribal authorities; and nongovernmental and private sector authorities. According to DHS, the National Incident Management System document is under review pending release of the revised National Response Plan, now the National Response Framework. The current version of the National Incident Management System document remains in effect during the 2007 hurricane season.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed the National Incident Management System, and the system defines the roles and responsibilities of various entities during emergency events. | Generally achieved |
| 6. Coordinate implementation of a national incident management system | *GAO findings:* Much more work remains for DHS to effectively coordinate implementation of the National Incident Management System. Drawing on our prior work identifying key practices for helping to enhance and sustain collaboration among federal agencies, key practices for collaboration and coordination include, among other things, defining and articulating a common outcome; establishing mutually reinforcing or joint strategies to achieve the outcome; identifying and addressing needs by leveraging resources; agreeing upon agency roles and responsibilities; establishing compatible policies, procedures, and other means to operate across agency boundaries; developing mechanisms to monitor, evaluate, and report the results of collaborative efforts; and reinforcing agency accountability for collaborative efforts through agency plans and reports. Homeland Security Presidential Directive 5 requires all federal departments and agencies to adopt and use the system in their individual preparedness efforts, as well as in support of all actions taken to assist state and local governments. However, in our work on Hurricane Katrina, we reported on examples of how an incomplete understanding of the National Incident Management System roles and responsibilities led to misunderstandings, problems, and delays. In Louisiana, for example, some city officials were unclear about federal roles. In Mississippi, we were told that county and city officials were not implementing the National Incident Management System because they did not understand its provisions. For more information, see GAO-06-618 and GAO-05-652.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on efforts to coordinate implementation of the National Incident Management System. DHS reported that in March 2004, it established the National Incident Management System Integration Center to coordinate implementation of the system. This center issues compliance guidelines to state and local responders annually and collects data on efforts to coordinate implementation of the National Incident Management System. DHS reported that more than 1 million state and local responders have taken training following guidelines established by the center for National Incident Management System compliance and that about 5.4 million students have received National Incident Management System-required training through the Emergency Management Institute as of February 2007. DHS also reported that the center, in conjunction with the Emergency Management Institute, released seven new National Incident Management System | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | training programs in fiscal year 2006, including courses on multiagency coordination, public information systems, and resource management, among others. DHS has also developed sample National Incident Management System-compliant tabletop, functional, and command post exercises for use by federal, state, and local government agencies in testing system policies, plans, procedures, and resources in emergency operations plans. In addition, the National Incident Management System specifies 34 requirements that state and local governments must meet to be compliant with the system, and as of October 1, 2006, all federal preparedness assistance administered by DHS became contingent on states' compliance with the system, including federal funding through the DHS Emergency Management Performance Grants, Homeland Security Grant Program, and Urban Area Security Initiative. DHS reported that during fiscal years 2005 and 2006, National Incident Management System requirements, including the completion of training, were based on a self-certification process. For fiscal year 2007, DHS reported that the self-certification process will not be used; rather DHS provided states a specific set of metrics for implementation of the National Incident Management System, and states are required to report on the establishment of these measurements.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. In fiscal years 2005 and 2006, states self-certified that they had met National Incident Management System requirements, and DHS has not fully verified the extent to which states were compliant with system requirements during those years. DHS has provided states with a specific set of metrics for fiscal year 2007, but the extent to which these metrics will enhance DHS's ability to monitor states' compliance with the National Incident Management System is not yet known. In addition, although DHS has taken actions, such as issuing compliance guidelines, providing training, developing sample exercises, and collecting data on implementation of the National Incident Management System, DHS did not provide us with documentation demonstrating how these actions have contributed to DHS's effective coordination of implementation of the system. For example, DHS did not provide us with documentation on how these training and exercise programs have contributed to ensuring effective coordination of National Incident Management System implementation. | |
| 7. Establish a single, all-hazards national response plan | *GAO findings:* DHS has established a single all-hazards national response plan, but the plan is undergoing revision. In December 2004, DHS issued the National Response Plan, which was intended to be an all-discipline, all-hazards plan establishing a single, comprehensive framework for the management of domestic incidents where federal involvement is necessary. The National Response Plan is applicable to incidents that go beyond the state and local levels and require a coordinated federal response, and the plan, operating within the framework of the National Incident Management System, provides the structure and mechanisms for national-level policy and operational direction for domestic incident management. The plan also includes a Catastrophic Incident Annex, which describes an accelerated, proactive national response to catastrophic incidents. DHS revised the National Response Plan following Hurricane Katrina, but we reported that these revisions did not fully address, or they raised new, challenges faced in implementing the plan. For more information, see GAO-06-618.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on efforts to establish an all-hazards national response plan. DHS reported that the National Response Plan is currently undergoing review and revision by federal, state, and local government officials; tribal authorities; and nongovernmental and private sector officials. According to DHS, this review includes all major components of the National Response Plan, including the base plan, Emergency Support Functions, annexes, and the role of the Principal Federal Official, Federal Coordinating Officer, and Joint Field Office Structure. A Catastrophic Planning Work Group is examining the Catastrophic Incident Annex and Supplement. DHS noted that this review is being conducted in four phases, with the first phase focused on prioritization of key issues, the second phase focused on the rewriting process, the third phase focused on releasing the revised documents, and the fourth phase focused on providing a continuous cycle of training, exercises, | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | and periodic reviews. DHS reported that, as of March 2007, it was in the rewriting phase and has gathered input on key issues from internal and external stakeholders, after-action reports, Hurricane Katrina reports, and other resources. According to DHS, the revised document is renamed the National Response Framework and was released to internal stakeholders for review at the end of July 2007. Based on the review, edits and updates will be made to the document prior to its anticipated release on August 20, 2007 for a 30 day public comment period. DHS reported that the current version of the National Response Plan document remains in effect during the 2007 hurricane season.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS issued the National Response Plan and a limited post-Katrina revision in May 2006, but we and others have identified concerns with those revisions. DHS also recognized the need for a more in-depth, substantive review and revision of the plan and expects to issue the latest revision in August 2007. DHS has acknowledged that some complex issues have taken more time than expected to assess and resolve. The changes made to the plan may affect roles and responsibilities under the plan and federal, state, and local agencies' training, exercises, and implementation plans. Until the National Response Plan and its annexes and Catastrophic Supplement are completed and distributed to all those with roles and responsibilities under the plan, federal agencies and others that have new or amended responsibilities under the revised plan cannot complete their implementation plans and the agreements needed to make the National Response Plan, its annexes, and supplements fully operational. | |
| 8. Coordinate implementation of a single, all-hazards response plan | *GAO and DHS IG findings:* Much more work remains for DHS to effectively coordinate implementation of the National Response Plan. Drawing on our prior work identifying key practices for helping to enhance and sustain collaboration among federal agencies, key practices for collaboration and coordination include, among other things, defining and articulating a common outcome; establishing mutually reinforcing or joint strategies to achieve the outcome; identifying and addressing needs by leveraging resources; agreeing upon agency roles and responsibilities; establishing compatible policies, procedures, and other means to operate across agency boundaries; developing mechanisms to monitor, evaluate, and report the results of collaborative efforts; and reinforcing agency accountability for collaborative efforts through agency plans and reports. In March 2006, the DHS IG reported on FEMA's disaster management activities in the wake of Hurricane Katrina. The DHS IG reported that during the response, several significant departures from National Response Plan protocols occurred: (1) DHS's actions to apply National Response Plan protocols for Incidents of National Significance and catastrophic incidents were ambiguous; (2) DHS defined a new, operational role for the Principal Federal Officer by assigning the officer both Federal Coordinating Officer and Disaster Recovery Manager authorities; and (3) the Interagency Incident Management Group took an operational role not prescribed in the National Response Plan. As a backdrop to these changes, the DHS IG reported that FEMA had not yet developed or implemented policies and training for roles and responsibilities necessary to supplement the National Response Plan. In reviewing DHS's response to Hurricanes Katrina and Rita, we also identified numerous weaknesses in efforts to implement the plan. For example, in the response to Hurricane Katrina, we reported in September 2006 that there was confusion regarding roles and responsibilities under the plan. DHS revised the National Response Plan following Hurricane Katrina, but we reported that these revisions did not fully address, or they raised new, challenges faced in implementing the plan. For more information, see GAO-06-618. Also, see Department of Homeland Security Office of Inspector General, *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina,* OIG-06-32 (Washington, D.C.: March 2006).<br>*DHS updated information:* In March 2007, DHS provided us with updated information on efforts to coordinate implementation of the National Response Plan. DHS reported that it developed and released training programs to support the National Response Plan and that this training has been required as a condition of certification of National Incident Management System | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | compliance by state and local governments. DHS also reported that it is revising the National Response Framework and intends to release the revised plan in August 2007.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS did not provide us with documentation on how its training programs have contributed overall to the department's efforts to coordinate implementation of the National Response Plan and could not demonstrate to us that the department has made progress in improving its ability to coordinate plan implementation since Hurricane Katrina. As we previously stated, the revised National Response Plan may require changes in federal, state, and local agencies' training, exercises, and implementation plans. It is also unclear how the revised plan will be implemented by states and first responders during the coming hurricane season, given that these entities will not have had an opportunity to train and practice under the revised version of the plan. We are concerned that if the revisions are not completed prior to the beginning of the 2007 hurricane season, it is unlikely that the changes resulting from these revisions could be effectively implemented for the 2007 hurricane season. | |
| 9. Develop a complete inventory of federal response capabilities | *GAO findings:* DHS has undertaken efforts related to development of an inventory of federal response capabilities, but did not provide us with evidence on the extent to which its efforts have resulted in the development of a complete inventory. In July 2005 we reported that DHS began the first stage of the capabilities-based planning process identifying concerns using 15 National Planning Scenarios that were developed by the Homeland Security Council. As it moved to the step in the process of developing a sense of preparedness needs and potential capabilities, DHS created a list of tasks that would be required to manage each of the 15 National Planning Scenarios. Then, in consultation with federal, state, and local emergency response stakeholders, it consolidated the list to eliminate redundancies and create a Universal Task List of over 1,600 discrete tasks. Next, DHS identified target capabilities that encompassed these critical tasks. From this universe of potential tasks, DHS worked with stakeholders to identify a subset of about 300 critical tasks that must be performed during a large-scale event to reduce loss of life or serious injuries, mitigate significant property damage, or are essential to the success of a homeland security mission. The final step of the first stage of DHS's planning process was to decide on goals, requirements, and metrics. To complete this step, DHS, working with its stakeholders, developed a Target Capabilities List that identified 36 capabilities needed to perform the critical tasks for the events illustrated by the 15 scenarios. In December 2005, DHS issued an updated version of the Target Capabilities List. For more information, see GAO-05-652.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to develop a complete inventory of federal response capabilities. For example, the Catastrophic Incident Supplement of the National Response Plan has been approved and includes identified specific capabilities from federal agencies that will be deployed according to a specified time frame in the event of a catastrophic incident (the Supplement may be revised based on the ongoing review of the National Response Plan and its annexes and supplements). DHS also reported that the National Incident Management System Incident Response Information System is currently undergoing development and testing. When testing is complete, the system will be provided to all federal agencies involved in the National Response Plan for collection of their inventory of National Incident Management System-typed resources. DHS reported that it is preparing to issue information to federal agencies that are signatories to the National Response Plan for agencies' use in creating an inventory of their resources. According to DHS, the database of these resources and capabilities is expected to be operational by the end of 2007. At this point, however, FEMA officials told us that the department does not have one comprehensive inventory of response capabilities. In addition, DHS reported that the Common Operating Picture Function in the Homeland Security Information Network serves as a communication tool that allows the DHS National Operations Center to gain real-time situational awareness of disaster response. During disaster response operations, automated reporting templates are populated by appropriate federal departments and agencies as specified under the | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | National Response Plan.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has taken a variety of steps to develop a complete inventory of federal response capabilities, including finalizing the National Response Plan Catastrophic Incident Supplement. DHS is also taking steps to develop the National Incident Management System Incident Response Information System, but has not yet released the system. While DHS provided us with information on its various tools for identifying and specifying federal capabilities that will be deployed in the event of an incident, DHS reported that it does not yet have a complete inventory of all federal capabilities. | |
| 10. Develop a national, all-hazards preparedness goal | *GAO findings:* DHS has developed an interim, national, all-hazards preparedness goal, but has not yet issued a final version of the goal. The December 2005 version of the National Preparedness Goal defines both the 37 major capabilities that first responders should possess to prevent, protect from, respond to, and recover from a wide range of incidents and the most critical tasks associated with these capabilities. We reported that an inability to effectively perform these critical tasks would, by definition, have a detrimental impact on effective protection, prevention, response, and recovery capabilities. For more information, see GAO-06-618 and GAO-05-652.<br>*DHS updated information:* In March 2007, DHS reported to us that public release of the final National Preparedness Goal was imminent, but did not provide us with a target time frame for issuing the final version of the goal. DHS officials noted that the department has worked with various federal, state, and local entities to develop, review, and get approval of the final National Preparedness Goal.<br>*Our assessment:* Until the final version of the National Preparedness Goal is issued, we conclude that DHS has generally not achieved this performance expectation. Although DHS has developed and issued an interim National Preparedness Goal, it has not yet issued a final version of the goal and did not provide a target time frame for doing so. Issuing a final version of the goal is important for finalizing the major capabilities required of first responders in preparing for and responding to various incidents. | Generally not achieved |
| 11. Support citizen participation in national preparedness efforts | *GAO findings and assessment:* We have not completed work on DHS's efforts to support citizen participation in national preparedness efforts, and DHS did not provide us with information on its actions to meet this performance expectation. As a result, we cannot make an assessment of DHS's progress for this performance expectation. | No assessment made |
| 12. Develop plans and capabilities to strengthen nationwide recovery efforts | *GAO and DHS IG findings:* DHS has faced challenges in developing plans and capabilities needed to strengthen nationwide recovery efforts.[a] In February 2006 we reported that beginning and sustaining community and economic recovery, including restoring a viable tax base for essential services, calls for immediate steps so residents can restore their homes and businesses. Removing debris and restoring essential gas, electric, oil, communications, water, sewer, transportation and transportation infrastructure, other utilities, and services such as public health and medical support are vital to recovery and rebuilding. However, these recovery efforts in the aftermath of Hurricane Katrina were hindered by various factors, including the magnitude and scope of the hurricane. For more information, see GAO-06-365R.<br>*DHS updated information:* In March and May 2007, DHS provided us with updated information on its efforts to develop plans and capabilities to strengthen nationwide recovery efforts. DHS and the American Red Cross developed the National Sheltering System to provide a Web-based data system to support shelter management and reporting and identification activities. DHS also issued a recovery strategy for mass sheltering and housing assistance in June 2006 to address contingencies for providing sheltering and housing assistance for declared emergencies and major disasters. FEMA also developed a Web-based Housing Portal to consolidate available rental resources for evacuees from federal agencies, private organization, and individuals. In | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | addition, DHS reported making enhancements to its debris removal processes by, for example, adjusting its debris removal policy to ensure cost sharing for federal contracting, establishing a list of debris removal contractors, and developing guidance for local government debris removal contractors. DHS reported that an interagency work group, initiated in 2005, is working to develop federal contaminated debris policy and operational procedure guidance. In addition, FEMA officials noted that the agency is using a cost estimating format to capture all costs for construction projects by taking into account allowances for uncertainties in the construction process.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS did not provide us with documentation on how its various initiatives have contributed overall to develop the department's capabilities to strengthen nationwide recovery efforts. DHS has taken steps to develop plans, policies, and guidance for recovery efforts. However, DHS did not provide us with evidence of its capabilities for recovery efforts. | |
| 13. Develop the capacity to provide needed emergency assistance and services in a timely manner | *GAO and DHS IG findings:* DHS has faced difficulties in developing the capacity to provide emergency services and assistance in a timely manner and has not provided us with documentation to demonstrate that it has effectively met this performance expectation. The various reports and our own work on FEMA's performance before, during, and after Hurricane Katrina suggested that FEMA's human, financial, and technological resources and capabilities were insufficient to meet the challenges posed by the unprecedented degree of damage and the resulting number of hurricane victims. Our work pointed out that the National Response Plan did not specify the proactive means or capabilities the federal government should use to conduct damage assessments and gain situational awareness when the responsible state and local officials were overwhelmed. As a result, response efforts were hampered by the federal government's failure to fully use its available assets to conduct timely, comprehensive damage assessments in Louisiana and Mississippi. With regard to logistics, our work and that of others indicated that logistics systems—the capability to identify, dispatch, mobilize, and demobilize and to accurately track and record available critical resources throughout all incident management phases—were often totally overwhelmed by Hurricane Katrina. Critical resources were not available, properly distributed, or provided in a timely manner. The result was duplication of deliveries, lost supplies, or supplies never being ordered. Reviews of acquisition efforts indicated that while these efforts were noteworthy given the scope of Hurricane Katrina, agencies needed additional capabilities to (1) adequately anticipate requirements for needed goods and services (2) clearly communicate responsibilities across agencies and jurisdictions and (3) deploy sufficient numbers of personnel to provide contractor oversight. For more information, see *Hurricanes Katrina and Rita: Unprecedented Challenges Exposed the Individuals and Households Program to Fraud and Abuse; Actions Needed to Reduce Such Problems in the Future,* GAO-06-1013, and GAO-06-618. Also, see Department of Homeland Security Office of Inspector General, *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina,* OIG-06-32 (Washington, D.C.: March 2006).<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to develop the capacity to provide needed emergency assistance and services in a timely manner. For example, DHS reported that FEMA and the American Red Cross have developed and improved methods to better identify and more quickly assist individuals evacuated to a shelter, including developing and implementing methods to identify and reunify missing and separated family members during a disaster. DHS reported that it has developed interim guidance regarding sending FEMA registration intake staff to Red Cross management shelters following a disaster and plan to refine a formal standard operating procedure for this activity. DHS also reported that it is pursuing contract and contingency surge capabilities that will allow for the rapid expansion of FEMA's registration intake capacity of up to 200,000 people per day. (FEMA surpassed 100,000 registrations per day following Hurricanes Katrina and Rita.) FEMA has also reported tripling its daily home inspection capacity through contracted firms from 7,000 to 20,000 per day. Furthermore, FEMA reported that it is working with federal, state, and | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | local partners to provide mass evacuee support planning to assist state and local governments in planning and preparing for hosting of large displaced populations. As part of these efforts, FEMA reported that it is working to develop an evacuee registration and tracking capability, implementation plans for federal evacuation support to states, and emergency sheltering guidance and planning assistance for potential host states and communities. FEMA reported that it plans to have a Mass Evacuation Management Unit operational by January 2008 and the National Mass Evacuation Registration and Tracking System operational once requirements are fully developed. In addition, DHS reported making enhancements to its logistics capabilities. For example, DHS has developed an Internet-based system that provides FEMA with the ability to manage its inventory and track the location of trailers carrying commodities. DHS officials also reported that the department is undertaking an optimization planning initiative to, among other things, identify best locations for logistics centers, but this planning effort is still in its early stages. DHS also reported that its Pre-Positioned Disaster Supply and Pre-Positioned Equipment Program provides equipment and supplies to emergency responders. DHS reported that its Mobile Emergency Response Support Detachments are equipped with communications capabilities to provide communication, logistics, operations, and power support for emergency responders and disaster victims.<br>*Our assessment:* We conclude that DHS generally has not achieved this performance expectation. Although DHS has taken actions to strengthen its capacity to provide emergency services and assistance, more work remains for DHS to achieve this performance expectation. For example, although DHS has reported making improvements to its logistics capabilities, its optimization planning efforts are still in the preliminary stages. Moreover, DHS did not provide us with documentation on how it determined requirements for the prepositioning of disaster supplies and equipment to assess whether FEMA has achieved its intended capacity. Furthermore, although DHS reported that it is working to develop various emergency assistance capabilities, such as evacuee registration, DHS generally did not provide us with documentation showing that these capabilities are currently in place and can provide needed services in a timely and accurate manner following an incident. In addition, none of DHS initiatives appear to have been tested on a scale that reasonably simulates the conditions and demand they would face following a major or catastrophic disaster. Thus, it is difficult to assess the probable results of these initiatives in improving response to a major or catastrophic disaster, such as a category 4 or 5 hurricane. | |
| 14. Provide timely assistance and services to individuals and communities in response to emergency events | *GAO and DHS IG findings:* DHS has faced difficulties in providing assistance and services to individuals and communities in a timely manner, particularly in response to Hurricanes Katrina and Rita. For example, each of the assessments of the federal government's response to Hurricanes Katrina and Rita we reviewed identified problems in FEMA's implementation of the Individuals and Households Program during and after the storms. Our review and our assessment of these reports showed that the agency's efforts to implement the program were hindered by a lack of planning, trained staff, and program limitations, despite its new and revised approaches for implementing the program. More broadly, we reported that although controls and accountability mechanisms help to ensure that resources are used appropriately, during a catastrophic disaster decision makers struggle with the tension between implementing controls and accountability mechanisms and the demand for rapid response and recovery assistance. On one hand, our work found many examples where quick action could not occur due to procedures that required extensive, time-consuming processes, delaying the delivery of vital supplies and other assistance. On the other hand, we also found examples where FEMA's processes under assistance programs to disaster victims left the federal government vulnerable to fraud and the abuse of expedited assistance payments. We estimate that through February 2006, FEMA made about $600 million to $1.4 billion in improper and potentially fraudulent payments to applicants who used invalid information to apply for expedited cash assistance. DHS and FEMA have reported a number of actions that are to be in effect for the hurricane season so that federal recovery programs would have more capacity to rapidly handle a catastrophic incident but also | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | provide accountability. Examples include significantly increasing the quantity of prepositioned supplies, such as food, ice, and water; placing global positioning systems on supply trucks to track their location and better manage the delivery of supplies; an enhanced phone system for victim assistance applications that can handle up to 200,000 calls per day; and improved computer systems and processes for verifying the eligibility of those applying for assistance. We reported that effective implementation of these and other planned improvements would be critical to achieving their intended outcomes. In March 2006, the DHS IG reported that while FEMA made major efforts to coordinate with other agencies and improve its ability to provide housing resources in its response to Hurricane Katrina, some of its efforts were more effective than others. For example, the DHS IG reported that FEMA and the Red Cross experienced difficulty in identifying the number and location of evacuees because both held different expectations for coordinating the mass care function. FEMA was slow in identifying and establishing its direct housing mission, so alternative housing resources, such as cruise ships, were initially used. Also, it was hard for FEMA to staff its Disaster Recovery Centers with experienced personnel, according to the DHS IG. In addition, the DHS IG reported that during the response to Hurricane Katrina, FEMA provided record levels of support to victims and emergency responders. Life-saving and life-sustaining commodities and equipment were delivered to the affected areas; personnel increased significantly in a short period of time to support response efforts and provide assistance to victims; and assistance was provided quickly in record amounts, sometime through innovative means. However, a lack of asset visibility in the resource-ordering process, inexperienced and untrained personnel, unreliable communications, and insufficient internal management controls demonstrated a continued need for improvement in how FEMA responds and delivers assistance, according to the DHS IG. For more information, see GAO-06-618, GAO-06-1013, and GAO-06-652. Also, see Department of Homeland Security Office of Inspector General, *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina,* OIG-06-32 (Washington, D.C.: March 2006).<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to provide timely assistance and services to individuals and communities in response to emergency events. For example, FEMA reported that it has developed new policies to ensure that all types of temporary housing options are able to be provided for displaced applicants with physical disabilities. FEMA also reported that it has developed updated policies to improve and expedite determination of applicant eligibility for the Individuals and Households Program and Expedited Assistance and has clarified policy on the appropriate authorization and use of emergency sheltering funds and individual housing assistance funds for disaster victims. DHS also reported taking steps to implement stronger controls in its registration and application processes for disaster assistance programs. For example, DHS reported deploying a new Internet registration application that does not allow duplicate registrations, adding identity proofing controls to the call center registration application for the Individuals and Households Program, and flagging applications in FEMA's database that fail identity proofing, are not residential addresses, or include at-risk Social Security numbers. In addition, DHS reported that it has five Mobile Registration Intake Centers that can be deployed to provide an on-site mechanism for disaster victims to register for FEMA assistance. According to DHS, these mobile centers have been tested several times, including in June 2006, in August 2006 during Tropical Storm Ernesto, and in April 2007. DHS reported that issues were identified during the earlier tests that indicated that improvements were needed, but noted that these issues have been resolved.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although DHS reported taking actions to provide timely assistance to individuals and communities, with appropriate safeguards against fraud and abuse, DHS did not provide us with documentation to demonstrate that these steps have improved the department's provision of assistance and services. For example, DHS did not provide us with documentation on the results of its provision of assistance and services to individuals affected by emergency incidents and | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | disasters since 2006. Furthermore, DHS did not provide with results of tests or exercises of its emergency assistance and service capabilities. For example, although DHS stated that it has resolved issues identified during tests of its Mobile Registration Intake Centers, DHS did not provide us with information on these issues or evidence that the issues have actually been resolved. | |
| 15. Implement a program to improve interoperable communications among federal, state, and local agencies | *GAO findings:* DHS has faced challenges in implementing a program to improve interoperable communications among federal, state, and local agencies. While DHS has implemented a program, referred to as SAFECOM, to improve interoperable communications, our past work showed that problems defining the scope, establishing performance goals and standards, and defining the roles of federal, state, local government and other entities were the three principal challenges to achieving effective interoperable communications for first responders. In April 2007 we reported that while SAFECOM is intended to improve interoperable communications at all levels of government, the objectives that the program has been working toward do not include improving interoperability between federal agencies and state and local agencies. For example, when conducting their baseline national survey of first responders to determine the current level of interoperability, program officials included state and local officials, but not federal officials. The survey included an extensive list of questions in which respondents were asked to rate interoperability (1) with other disciplines, (2) with other jurisdictions, and (3) between state and local governments. Respondents were also asked at the end of the survey to list federal agencies they interoperate with; however, no effort was made to gauge the level of interoperability with the federal government, as had been done for other disciplines and jurisdictions and between state and local governments. In lieu of having communications systems that enable direct interoperability between federal first responders and state and local first responders, first responders have resorted to alternative means of communicating. For example, state or local agencies may loan radios to federal first responders or physically pair a federal first responder with a state or local responder so they can share information and relay it back to their agencies. While approaches such as these may be effective in certain situations, they can reflect a general lack of planning for communications interoperability. We reported that using “work-arounds” such as these could reduce the efficiency and effectiveness of the overall public safety response to an incident. SAFECOM officials stated that the program’s focus has been on state and local agencies because they consider them to be a higher priority. Further, while they stated that it would be possible for federal agencies to make use of some of the planning tools being developed primarily for state and local agencies, SAFECOM has not developed any tools that directly address interoperability with federal agencies. However, interoperability with federal first responders remains an important element in achieving nationwide interoperability. We reported that until a federal coordinating entity such as SAFECOM makes a concerted effort to promote federal interoperability with other governmental entities, overall progress in improving communications interoperability will remain limited. For more information, see *Project SAFECOM: Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration,* GAO-04-494 and *First Responders: Much Work Remains to Improve Communications Interoperability,* GAO-07-301.<br>*DHS updated information:* In March and June 2007, DHS provided us with information on its efforts to implement a program for improving interoperable communications. For example, DHS established the Office for Interoperability and Compatibility, of which SAFECOM is a part, to strengthen and integrate interoperability and compatibility efforts. DHS also reported that SAFECOM is developing tools, templates, and guidance documents for interoperability, including field-tested statewide planning methodologies, online collaboration tools, communications requirements, and an online library of lessons learned and best practices. The department established the Office of Emergency Communications to administer the responsibilities and authorities of SAFECOM, the Interoperable Communications Technical Assistance Program, and the Integrated Wireless Network, which are three programs focused on improving interoperable communications. According to DHS, the mission of the Office of Emergency Communications is | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | to support and promote the ability of emergency response providers and government officials at the local, tribal, state, and federal levels to continue to communicate in the event of disasters or acts of terrorism, and to ensure, accelerate, and attain emergency interoperable communications nationwide. Moreover, DHS noted that its focus on state and local interoperable communications is proportional to the nature of the interoperability problem, as there are over 50,000 emergency response agencies at the state and local level and 90 percent of communications infrastructure is owned and operated at the state level. With regard to federal agencies, DHS noted that SAFECOM has and will continue to partner with federal agencies, such as the Departments of Justice and Defense, and that DHS participates in the Federal Partnership for Interoperable Communications, which is charged with addressing federal wireless communications interoperability. In addition, DHS noted that is it in the process of conducting a baseline assessment evaluating interoperable capabilities for all departments and agencies.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. While DHS has made progress in implementing a program to improve interoperable communications, these implementation efforts have focused primarily on improving interoperability among state and local entities, and DHS is in the process of evaluating federal agencies' interoperable communications' capabilities through the recently established Office of Emergency Communications. DHS did not provide us with documentation on the extent to which it has taken actions to improve interoperability with federal agencies, which we reported is a key part of communications interoperability. Moreover, while, SAFECOM officials stated that the program's focus has been on state and local agencies because there are more state and local first responder agencies and most of the communications infrastructure is owned by state and local agencies, interoperability with federal first responders remains an important element in achieving nationwide interoperability and is part of SAFECOM's tasking under the Intelligence Reform and Terrorism Prevention Act of 2004. As we previously reported, until a more concerted effort is made to promote federal interoperability with other governmental entities, overall progress in improving communications interoperability would remain limited. | |
| 16. Implement procedures and capabilities for effective interoperable communications | *GAO findings:* DHS has faced difficulties in implementing procedures for effective interoperable communications. In April 2007, we reported that SAFECOM—a DHS program intended to strengthen interoperable public safety communications at all levels of government—has provided planning tools to state and local governments intended to help states and local agencies improve their procedures and capabilities to enable effective interoperable communications. However, based on our review of four states and selected localities, SAFECOM's progress in achieving its goals of helping these states and localities improve interoperable communications has been limited. We often found that the states and local jurisdictions either did not find the tools useful or were unaware that the tools existed. These state and local officials did not find the tools and guidance useful for various reasons, including that (1) the tools and guidance are too abstract and do not provide practical implementation guidance on specific issues; (2) the documents are lengthy and hard to use as reference tools; and (3) awareness of SAFECOM and its tools has not reached all state and local agencies. To its credit, SAFECOM's Interoperability Continuum—which is intended to provide a framework that emergency response agencies can use to baseline their planning and implementation of interoperability solutions—was the most widely used and recognized of its tools. Seven of the 15 states and localities we visited indicated that they used the continuum to assess their interoperability status and plan improvements. Another initiative that had a significant impact was the Regional Communications Interoperability Pilot. Officials from Kentucky—one of the two states that participated in the pilot—indicated that the pilot was very helpful in facilitating communications planning by identifying relevant stakeholders and bringing those stakeholders together for extended discussions about interoperability. In April 2007 we reported that one factor contributing to the limited impact that SAFECOM has had on implementing procedures and capabilities to enable effective interoperable communications, is that its activities have not been guided by a program plan. A program plan is a critical tool to ensure a program meets its goals and responsibilities. Such a tool is used to align planned | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
|  | activities with program goals and objectives, as well as define how progress in meeting the goals will be measured, compared, and validated. Rather than using a program plan to guide their activities, SAFECOM officials stated that they develop tools and guidance based on a list of suggestions obtained from first responders. The SAFECOM Executive Committee—a steering group composed of public safety officials from across the country—prioritized the list of suggestions, but this prioritization has not been used to develop a plan. Instead, program officials have made ad hoc decisions regarding which suggestions to implement based on executive committee input, as well as the difficulty of implementation. We reported that while this approach incorporates a degree of prioritization from first responders, it does not provide the structure and traceability of a program plan. For more information, see *Homeland Security: Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications,* GAO-04-740 and GAO-07-301.<br>*DHS updated information:* In March and June 2007, DHS provided us with information on its efforts to implement policies and procedures for effective interoperable communications. DHS reported that it developed the Statement of Requirements to define operational and functional requirements for emergency response communications and the Public Safety Architecture Framework to help emergency response agencies map interoperable communications system requirements and identify system gaps. DHS also reported that it developed the Statewide Communications Interoperability Planning Methodology to assist states in initiating statewide interoperability planning efforts and that it is helping states develop their interoperability plans by the end of 2007. DHS reported that SAFECOM's guidance and tools are driven by and incorporate the input of emergency responders and that its Interoperability Continuum is, for example, widely used as the model framework for defining and addressing the problem of interoperability. In addition, DHS reported that it is conducting a national baseline assessment to, among other things, define the range of interoperable and emergency capabilities needed; assess the current available capabilities to meet needs; identify the gap between current capabilities and defined requirements; and include a national interoperable emergency communications inventory to identify requirements for federal agencies. DHS noted that the Office of Emergency Communications will develop a National Emergency Communications Plan in fiscal year 2008 and is in the process of developing a strategic plan for fiscal years 2008 through 2013.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. As we previously reported, officials from selected states and localities often found that the key tools DHS issued such as the Statement of Requirement and the Public Safety Architecture Framework which are intended to provide capabilities and procedures to state and local agencies to help enable effective interoperable communications were not helpful, or officials were unaware of what assistance the program had to offer. We also found that DHS does not have performance measures in place to determine how effective these tools are and to make improvements based on feedback. |  |
| 17. Increase the development and adoption of interoperability communications standards | *GAO findings:* More work remains for DHS to increase the development and adoption of interoperability communications standards. In April 2007 we reported that until recently, little progress had been made in developing Project 25 standards—a suite of national standards that are intended to enable interoperability among the communications products of different vendors. We reported that although one of the eight major subsets of standards was defined in the project's first 4 years (from 1989 to 1993), from 1993 through 2005, no additional standards were completed that could be used by a vendor to develop elements of a Project 25 compliant system. Over the past 2 years, progress has been made in developing specifications for three additional subsets of standards. However, we reported that ambiguities in the published standards have led to incompatibilities among products made by different vendors, and no formal compliance testing has been conducted to ensure vendors' products are interoperable. More recently, informal peer testing among vendors has occurred. To address the lack of well-defined standards, users and manufacturers have been revising the standards. To address the issue of a lack of formal | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | compliance testing, SAFECOM, the National Institute of Standards and Technology, and the Project 25 steering committee, began developing a peer compliance assessment program for Project 25 products in April 2005. We reported that this compliance assessment program is to use various vendors' approved laboratories to test Project 25 systems through a set of agreed-upon tests that will validate that the systems from various vendors can successfully interoperate and meet conformance and performance requirements. According to the National Institute of Standards and Technology, the vendors will be expected to conduct the tests in compliance with a handbook on general testing procedures and requirements, which the National Institute of Standards and Technology is preparing to publish. For more information, see GAO-07-301. Also, see Department of Homeland Security Office of Inspector General, *Review of DHS' Progress in Adopting and Enforcing Equipment Standards for First Responders,* OIG-06-30 (Washington, D.C.: March 2006).<br>*DHS updated information:* In March 2007, DHS reported that it has helped to develop initial standards for six of the eight major system interfaces associated with Project 25, a suite of standards for interoperability. In June 2007, DHS reported that its Office of Emergency Communications is to establish requirements for interoperable communications capabilities in coordination with the Office for Interoperability and Compatibility. DHS reported that it has worked to promote the acceleration, completion, and deployment of interoperable communications standards, but noted that DHS does not have the authority to set standards. Specifically, DHS reported that it has worked with the National Institute of Standards and Technology to establish a vision and key priorities for standards and that the Project 25 standards should be completed within 18 to 24 months.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. In our prior work, we reported that there were ambiguities in published standards, which led to incompatibilities among products made by different vendors. DHS has taken some steps to address these challenges, but the effectiveness of these efforts is unclear. Moreover, DHS reported that it has worked with its partners to develop the Project 25 standards but, according to DHS, completion of these standards is many months away. | |
| 18. Develop performance goals and measures to assess progress in developing interoperability | *GAO findings:* DHS has not yet developed a sufficient set of performance goals and measures to effectively assess progress in developing interoperability. For instance, in April 2007 we reported that since 2001, the management and goals of the SAFECOM program have changed several times. In 2003, the SAFECOM program was transferred to the Office of Interoperability and Compatibility within the Directorate of Science and Technology in DHS and is now within the Office of Emergency Communications.[b] Its goals included increasing interoperable communications capacity of local, tribal, and state public safety agencies, and increasing the number of states that have initiated or completed statewide plans. However, these goals do not include improving interoperability between federal agencies and state and local agencies which is part of SAFECOM's tasking in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004. With regard to establishing performance measures, we reported that SAFECOM program officials have established six performance measures to assess progress, including the percentage of fire, emergency medical services, and law enforcement organizations that have established informal interoperability agreements with other public safety organizations; the percentage of public safety agencies that report using interoperability to some degree in their operations; the percentage of states that have completed statewide interoperability plans; the percentage of grant programs for public safety communications that include SAFECOM guidance; and the amount of reduction in the cycle time for national interoperability standards development. However, we noted that several key aspects of the program are not being measured. For example, one of the program's goals is to increase the development and adoption of standards. However, the only associated performance measure is reduction in the cycle time for national interoperability standards development—not the extent to which adoption of standards has increased or whether interoperability is being facilitated. Also, in assessing the growth of interoperable communications capacity at local, tribal, and state public | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | safety agencies, SAFECOM's measures—the percentage of states that have established informal interoperability agreements with other public safety organizations and the percentage of public safety agencies that report using interoperability to some degree in their operations — addresses only two of the five areas that SAFECOM has defined as key to improving interoperability (it does not assess improvements made in governance, technology, or training). Moreover, none of the program's measures assess the extent to which the first responder community finds the tools and assistance helpful or the effectiveness of program outreach initiatives. Consequently, we reported that measures of the effectiveness of the program and areas for improvement are not being collected and are not driving improvements in the program, contributing to its limited impact. According to SAFECOM officials, by mid-2007, they plan to establish a measure to assess customer satisfaction. We reported that until DHS develops and implements a program plan that includes goals focusing on improving interoperability among all levels of government, establishes performances measures that determine if key aspects of the SAFECOM program are being achieved, and assesses the extent to which the first responder community finds the tools and assistance helpful, the impact of its efforts to improve interoperable communications among federal, state, and local agencies will likely remain limited. For more information, see GAO-07-301.<br>*DHS updated information:* In March 2007, DHS reported that SAFECOM has goals for improving interoperability among federal, state, local, and tribal agencies. It also reported that SAFECOM, with the Office of Management and Budget, adopted a strategy, with metrics, based on user needs to meet its mission as an e-government project. DHS also reported that it is working to establish quantifiable performance measures by the third quarter of 2007. In addition, DHS reported that its Office of Emergency Communications has initiated a program planning and performance measurement initiative to incorporate and build upon past performance measures established by SAEFCOM and the Office of Management and Budget.<br>*Our assessment:* We conclude that DHS generally has not achieved this performance expectation. While DHS officials indicate that the Office Emergency Communications plans to better address this performance expectation, the office is not yet operational. For example, this office was required to provide Congress with an initial plan for establishing this office by February 1, 2007, and as of June this plan was not yet complete. In our prior work, we reported that while DHS established performance measures for the SAFECOM program, key aspects of the program were not being measured. We also reported that none of the program's measures assess the extent to which first responders find DHS tools and assistance helpful or the effectiveness of outreach initiatives. | |
| 19. Provide grant funding to first responders in developing and implementing interoperable communications capabilities | *GAO findings:* DHS has provided grant funding to first responders for developing and implementing interoperable communications. In April 2007 we reported according to DHS, $2.15 billion in grant funding was awarded to states and localities from fiscal year 2003 through fiscal year 2005 for communications interoperability enhancements. This funding, along with technical assistance, has helped to make improvements on a variety of specific interoperability projects. We reported that one of the main purposes of the DHS grants program is to provide financial assistance to states and localities to help them fund projects to develop and implement interoperable communications systems. We reported that, according to SAFECOM guidance, interoperability cannot be solved by any one entity alone and, therefore, an effective and interoperable communications system requires a clear and compelling statewide strategy focused on increasing public safety effectiveness and coordination across all related organizations. A statewide interoperability plan is essential for outlining such a strategy. We reported that the narrow and specific use of DHS funding in the states we reviewed could be traced in part to the lack of statewide plans; interoperability investments by individual localities have not been coordinated toward achieving a broader goal for the state. We reported that in accordance with a previous recommendation, DHS has required grant recipients to develop and adopt a statewide communications plan by the end of 2007. Additionally, the fiscal year 2007 DHS appropriations act states that DHS may restrict funding to a state if it does not submit a | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | statewide interoperable communication plan. However, despite our other previous recommendation that DHS should require that states certify that grant applications be consistent with statewide plans, no process has yet been established for ensuring that states' grant requests are consistent with their statewide plans and long-term objectives for improving interoperability. We noted that DHS Grants and Training officials were considering instituting such a process but they did not yet have specific plans to do so. We reported that because of the lack of coordination, state and local governments were investing significant resources, including DHS grant funds, in developing independent interoperability solutions that do not always support each others' needs. Until the DHS-mandated statewide communications plans are in place, and processes have been established for ensuring that each state's grant request is consistent with its statewide plan and longer-term interoperability goals, progress by states and localities in improving interoperability is likely to be impeded. We also reported that in addition to statewide plans, an overarching national plan is critical to coordinating interoperability spending, especially where federal first responders are involved. For more information, see GAO-07-301.<br>*DHS updated information:* In March 2007, DHS reported that SAFECOM had developed coordinated grant guidance that is required for all grant programs that provide federal funds for interoperable communications. DHS also reported that it is working to ensure all grant funding is tied to statewide interoperable communications plans.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation, as the department has provided grant funding to first responders for developing and implementing interoperable communications capabilities. | |
| 20. Provide guidance and technical assistance to first responders in developing and implementing interoperable communications capabilities | *GAO findings:* While DHS has provided some guidance and technical assistance, the usefulness of these efforts varies. For example, based on a previous review of four states and selected localities, we often found that the selected states and local jurisdictions either did not find key tools useful or were unaware that the tools existed. Selected state and local officials did not find the tools and guidance useful for various reasons, including that (1) the tools and guidance are too abstract and do not provide practical implementation guidance on specific issues; (2) the documents are lengthy and hard to use as reference tools; and (3) awareness of SAFECOM and its tools has not reached all state and local agencies. As we previously reported, recently, SAFECOM has issued additional tools and guidance for state and local agencies to use, however, we were unable to assess them during our previous review because these tools were still new and we did not receive assessments of them from state and local officials. To its credit, as we reported in April 2007, the Interoperable Communications Technical Assistance Program, which is intended to provide on-site assistance to Urban Area Security Initiative areas to, among other things, assist with developing tactical interoperability plans, planning exercises, assessing communication gaps, and designing interoperable systems, had been beneficial to each of the four Urban Area Security Initiative areas we visited. DHS provided extensive assistance to the urban areas in developing their tactical interoperability communications plans, However, DHS curtailed the exercises that each urban areas was required to conduct to validate the robustness and completeness of their plans. Due to the complexity of these exercises, the Urban Area Security Initiative areas were originally allotted 12 months to plan and execute robust, full-scale exercises; DHS subsequently reduced this to 5 months. DHS officials indicated that they accelerated the deadline so that they could use the results as inputs into the interoperability scorecards that they published in January 2007. To compensate for the reduced time frame, DHS reduced the requirements of the full-scale exercise, advising the Urban Area Security Initiative areas to limit the scope and size of their activities. In reducing the scope of their exercises, the Urban Area Security Initiative areas had to reduce the extent to which they tested the robustness and effectiveness of their interoperability plans. Without robust exercises to validate tactical interoperability communications plans, the Urban Area Security Initiative areas can only have limited confidence in the plans' effectiveness, and thus the value of DHS's efforts may continue to be limited. Similarly, the constraints placed on the exercises means that DHS's scorecards of each of the Urban Area Security Initiative areas are based on questionable data. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | In addition, we reported that SAFECOM's activities have focused primarily on providing planning tools to state and local governments. For more information, see GAO-07-301.<br>*DHS updated information:* In March 2007, DHS reported that it has developed a variety of guidance documents related to interoperability. These documents include the Statewide Communications Interoperability Planning Methodology and Brochure; Tabletop Methodology; State Planning Guidebook; Migration Model; and guides on a creating a charter, writing a memorandum of understanding, writing standard operating procedures, standards and technology, and procurement. DHS also reported that by the end of fiscal year 2007, all states and territories are to develop and adopt a Statewide Communications Interoperability Plan to be reviewed by the Office of Emergency Communications. DHS reported that it will provide technical assistance to states and territories in the development of their plans through the Interoperable Communications Technical Assistance Program. Moreover, DHS reported that it has provided various assistance to state and local jurisdictions through the Interoperable Communications Technical Assistance Program, including providing assistance in the development Tactical Interoperable Communication Plans for 65 metropolitan areas; participating in the plans' exercise validation; and developing and providing assistance to jurisdictions in using the Communication and Asset Survey Mapping Tool. In addition, DHS reported that SAFECOM is in the process of developing performance measures to ensure its tools are being used throughout the emergency response community.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has provided various guidance and technical assistance to first responders in developing and implementing interoperable communications. However, as we recently reported, several states and localities were not aware of SAFECOM tools and guidance and did not find the tools and guidance useful. In addition, DHS reported that it is developing performance measures to assess use of its tools and guidance, but the department has not yet developed these measures. | |
| 21. Provide assistance to state and local governments to develop all-hazards plans and capabilities | *GAO and DHS IG findings:* Although DHS has taken actions to provide assistance to state and local governments, this assistance has not always focused on the development of all-hazards plans and capabilities. In July 2005 we reported that because terrorist attacks share many common characteristics with natural and accidental disasters, many of the capabilities first responders need to support national preparedness efforts are similar. Our analysis of DHS's Target Capabilities List and our discussions with first responders and other emergency management stakeholders revealed that the capabilities required to address terrorist attacks and to address natural and accidental disasters are most similar for protection, response, and recovery, and differ most for prevention. More specifically at the time of our review, 30 of the 36 target capabilities yielded by DHS's capabilities based planning process applied across all types of emergency events. It is possible that terrorist attacks could be prevented through actionable intelligence (i.e., information that can lead to stopping or apprehending terrorists), but there is no known way to prevent natural disasters, such as hurricanes, earthquakes, and tornadoes. Natural or accidental disasters differ from terrorist attacks in that they are unintentional and unplanned rather than the result of deliberate, planned action. It is the deliberate, planned nature of terrorist attacks that makes preventive efforts for such attacks principally the responsibility of intelligence and law enforcement agencies. In 2005 we also reported that DHS grant programs have largely focused on enhancing first responders' capabilities to respond to terrorist attacks based on Homeland Security Presidential Directive 8 and legislation that emphasize preparedness assistance for catastrophic terrorism as the highest priority for federal funding. The priorities of some first responders we interviewed did not align with DHS's priorities for enhancing capabilities. For example, during our interviews, 31 of 39 first responder departments who replied to a question about DHS's training programs, exercise activities, and grant funds disagreed that these were focused on all-hazards. In addition, officials from four first responder departments went on to say that DHS required too much emphasis on terrorism-related activities in requests for equipment and training—for example, combating | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | weapons of mass destruction and preventing and responding to terrorist attacks using chemical, biological, radiological, nuclear, and explosive materials. However, responders said that they had a greater need for assistance preparing for natural and accidental disasters. During our interviews, 37 of the 69 first responder departments who responded to a question about the programmatic challenges they face cited the need for additional flexibility from DHS or state agencies in order to use grant funds to enhance their ability to respond to events that were more likely to occur in their jurisdictions. In March 2006, the DHS IG reported that the response to Hurricane Katrina demonstrated that DHS's efforts to protect and prepare the nation for terrorist events and natural disasters had not yet translated into preparedness for all hazards. State emergency management staff interviewed said the majority of DHS preparedness grants were spent on terrorism preparedness, which had not afforded sufficient support or funding for natural hazards preparedness. Staff in the Hurricane Katrina affected states described a heavy emphasis on terrorism funding and expressed bafflement at the lack of natural hazards funding. Few perceived grants as "all-hazard." The DHS IG reported that this perception may have been fueled by the fact that all DHS preparedness grants were managed by an entity—the former Office of Domestic Preparedness—whose mandate was originally terrorism preparedness. Additionally, only 2 of the 15 National Planning Scenarios, a compilation of potential disasters developed to support preparedness, involved natural disasters (a major hurricane and a major earthquake). The DHS IG found that although the documents in the National Preparedness System addressed all hazards, the prevalence of terrorism-related items in them fostered a perception that the preparedness for and response to a terrorist event is different from that of a naturally occurring event. Further, the DHS IG reported that requirements associated with federal emergency preparedness grants to states also supported the perception that terrorism preparedness is separate from natural disaster preparedness. A majority of grants to states emphasized preparedness for terrorism and weapons of mass destruction and limited use of the grants to terrorism-preparedness measures, such as the purchase of specific personal protective equipment. Office of Domestic Preparedness staff said that state grantees were failing to take advantage of the grants' flexibility and use them for all-hazards preparedness measures. State emergency managers questioned grant packages that required so much spending on potential events involving terrorism and weapons of mass destruction, when they received far less funding to prepare for natural disasters that are certain to recur. For example, the DHS IG found that the Gulf Coast region experienced 91 major disaster and emergency declarations from September 1, 1995, to September 1, 2005, all due to natural hazards such as hurricanes and flooding. Yet a significant portion of the federal funding for these states was earmarked for terrorism preparedness to the exclusion of natural hazards preparedness. For more information, see GAO-05-652 and *Homeland Security: Management of First Responder Grant Programs and Efforts to Improve Accountability Continue to Evolve,* GAO-05-530T. Also, see Department of Homeland Security Office of Inspector General, *A Performance Review of FEMA's Disaster Management Activities in Response to Hurricane Katrina,* OIG-06-32 (Washington, D.C.: March 2006). | |
| | *DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to provide assistance to state and local governments in developing all-hazards plans and capabilities. For example, DHS reported that its Office of Grants and Training conducted a series of mobile implementation training team interviews with senior state and local officials to facilitate the development of state and local all-hazards plans and capabilities. This office also completed the Nationwide Plan Review, a national review of preparedness planning following Hurricane Katrina. Moreover, DHS reported that FEMA's Mitigation Division provides assistance to communities in the development of hazard mitigation plans that include hazard identification and risk assessment and identification and prioritization of potential mitigation measures. DHS noted that the Mitigation Division reviews and approves these plans. DHS reported that FEMA has approved over 13,500 community hazard mitigation plans, 54 tribal hazard mitigation plans, 50 state hazard mitigation plans, and 11 state enhanced hazard mitigation plans as of March 2007. In addition, FEMA reported that is has provided grants totaling over $110 million (since | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | 2002) to fund the development of more than 1,500 state and local hazard mitigation plans through the Hazard Mitigation Grant Program and the Pre-Disaster Mitigation Grant Program.<br>*Our assessment:* We conclude that DHS generally has not achieved this performance expectation. DHS did not provide us with evidence on the extent to which its assistance to state and local governments has focused on all-hazards, rather than just terrorism preparedness and response or hazard mitigation. DHS also did not provide us with documentation that its assistance to state and local governments has helped these government agencies develop all-hazards capabilities, in addition to hazard mitigation plans. | |
| 22. Administer a program for providing grants and assistance to state and local governments and first responders | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has developed and is administering programs for providing grants and assistance to state and local governments and first responders. DHS provides grant funds to the 50 states, the District of Columbia, the Commonwealths of Puerto Rico and the Northern Mariana Islands, American Samoa, the Virgin Islands, Guam, and selected urban areas. For more information, see *Homeland Security: Management of First Responder Grant Programs Has Improved, but Challenges Remain,* GAO-05-121 and GAO-05-652. | Generally achieved |
| 23. Allocate grants based on assessment factors that account for population, critical infrastructure, and other risk factors | *GAO findings and assessment:* DHS has taken actions to allocate grants based on assessment factors that account for population, critical infrastructure, and other risk factors, and we conclude that DHS has generally achieved this performance expectation. 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 Urban Area Security Initiative 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. For more information, see GAO-07-386T and *Homeland Security Grants: Observations on Process DHS Used to Allocate Funds to Selected Urban Areas,* GAO-07-381R. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 24. Develop a system for collecting and disseminating lessons learned and best practices to emergency responders | *GAO findings:* DHS has taken actions to develop a system to effectively collect and disseminate lessons learned and best practices to emergency responders, but more work remains. DHS has established the Lessons Learned Information Sharing online portal. The portal states that it seeks to improve preparedness nationwide by allowing local, state, and federal homeland security and response professionals to access information on the most effective planning, training, equipping, and operating practices for preventing, preparing for, responding to, and recovering from acts of terrorism. However, we reported in December 2006 that although the Lessons Learned Information Sharing portal includes guidance and other emergency preparedness information, officials from two of the five major cities and two of the four states we visited told us that specific information is not easy to find, in part, because the portal is difficult to navigate. Upon using the portal, we also found this to be true. For example, the search results appeared to be in no particular order and were not sorted by date or relevant key terms, and searched terms were not highlighted or shown anywhere in the abstracts of listed documents. In addition, some studies were not available through the portal, including studies from some of the experts with whom we have spoken and who provided us with useful information on evacuation preparedness for transportation-disadvantaged populations. In commenting on our December 2006 report, DHS officials told us that they had improved the overall functionality of DHS's Lessons Learned Information Sharing portal. We revisited the portal as of December 7, 2006, and it appeared to have improved some of its search and organizational functions. We have found, however, that some of the issues we previously identified still remained, including, when using the portal's search function, no direct link to key evacuation preparedness documents, such as DHS's Nationwide Plan Review Phase I and II reports. For more information, see *Transportation-Disadvantaged Populations: Actions Needed to Clarify Responsibilities and Increase Preparedness for Evacuations,* GAO-07-44 and GAO-05-652.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to collect and disseminate lessons learned and best practices to emergency responders. DHS reported that its Lessons Learned Information Sharing System houses over 400 after-action reports; 1,200 emergency operations plans; and 500 lessons learned and best practices that are shared among the system's more than 31,000 members. DHS reported that in a survey of system users conducted in June 2006, 86 percent reported being "satisfied" or "very satisfied" with the information provided. In addition, DHS reported that it is working to improve the functionality of the Lessons Learned Information Sharing System and that enhancements to the system, including an improved search engine, is expected to be implemented by the end of September 2007.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although DHS has developed and implemented the Lessons Learned Information Sharing System, it is not clear that this system is effectively collecting and disseminating lessons learned and best practices to emergency responders. In addition, DHS is taking some actions to address the issues with the Lessons Learned Information Sharing System that we previously identified, but these actions are not yet complete. | Generally not achieved |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

[a] We refer to DHS's recovery efforts as the development, coordination, and execution of service and site restoration plans through DHS assistance programs.

[b] The Post-Katrina Emergency Management Reform Act of 2006, Pub. L. No. 109-295, tit. VI, 120 Stat. at 1394-62, transferred the responsibilities for administering SAFECOM to the Office of Emergency Communications, which is under the Office of Cyber Security and Communications within the Directorate for National Protection and Programs. The Office for Interoperability and Compatibility retained responsibility for research, development, testing, evaluation, and standards-related elements of SAFECOM. See id., § 671(b).

## DHS Has Made Moderate Progress in Strengthening the Protection of Critical Infrastructure and Key Resources

Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, and national public health or safety, or any combination of these matters. Key resources are publicly or privately controlled resources essential to minimal operations of the economy or government, including individual targets whose destruction would not endanger vital systems but could create a local disaster or profoundly damage the nation's morale or confidence. While the private sector owns approximately 85 percent of the nation's critical infrastructure and key resources, DHS has wide-ranging responsibilities for leading and coordinating the overall national critical infrastructure and key resources protection effort.

The *National Infrastructure Protection* Plan identifies 17 critical infrastructure and key resources sectors:

- agriculture and food;
- banking and finance;
- chemical;
- commercial facilities;
- commercial nuclear reactors, materials, and waste;
- dams;
- defense industrial base;
- drinking water and water treatment systems;
- emergency services;
- energy;
- government facilities;
- information technology;
- national monuments and icons;
- postal and shipping;
- public health and healthcare;
- telecommunications; and
- transportation systems.

DHS has overall responsibility for coordinating critical infrastructure and key resources protection efforts.[26] Within DHS, the Office of Infrastructure Protection has been designated as the Sector-Specific Agency[27] responsible for the chemical; commercial facilities; dams; emergency services; and commercial nuclear reactors, materials, and waste sectors. TSA has been designated as the Sector-Specific Agency for postal and shipping, and TSA and the Coast Guard have been designated the Sector-Specific Agencies for transportation systems. The Federal Protective Service within ICE has been designated as the Sector-Specific Agency for government facilities. The Office of Cyber Security and Telecommunications has been designated the Sector-Specific Agency for Information Technology and Telecommunications.

As shown in table 30, we identified seven performance expectations for DHS in the area of critical infrastructure and key resources protection, and we found that overall DHS has made moderate progress in meeting those performance expectations. Specifically, we found that DHS has generally achieved four performance expectations and has generally not achieved three others.

[26] Other departments have major roles in critical infrastructure and key resource protection as well. For example, the Department of Defense is active in this mission area, primarily in areas of physical security of military and military-related activities, installations, and personnel. The Department of Energy's role involves the development and implementation of policies and procedures for safeguarding the nation's power plants, research labs, weapons production facilities, and cleanup sites from terrorists. The Department of Justice, primarily through work done by the Federal Bureau of Investigation and the Computer Crime and Intellectual Property Section of the Criminal Division, is active in this mission area in preventing, where possible, the exploitation of the Internet, computer systems, or networks as the principal instruments or targets of terrorist organizations.

[27] The National Infrastructure Protection Plan defines the responsibility of Sector-Specific Agencies as to implement the plan's framework and guidance as tailored to the specific characteristics and risk landscapes of each of the critical infrastructure and key resources sectors designated in Homeland Security Presidential Directive 7.

Table 30: Performance Expectations and Progress Made in Critical Infrastructure and Key Resources Protection

| | Assessment | | |
|---|---|---|---|
| Performance expectation | Generally achieved | Generally not achieved | No assessment made |
| 1. Develop a comprehensive national plan for critical infrastructure protection | ✓ | | |
| 2. Develop partnerships and coordinate with other federal agencies, state and local, governments, and the private sector | ✓ | | |
| 3. Improve and enhance public/private information sharing involving attacks, threats, and vulnerabilities | | ✓ | |
| 4. Develop and enhance national analysis and warning capabilities for critical infrastructure | | ✓ | |
| 5. Provide and coordinate incident response and recovery planning efforts for critical infrastructure | | ✓ | |
| 6. Identify and assess threats and vulnerabilities for critical infrastructure | ✓ | | |
| 7. Support efforts to reduce threats and vulnerabilities for critical infrastructure | ✓ | | |
| **Total** | **4** | **3** | **0** |

Source: GAO analysis.

Note: An assessment of “generally achieved” indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of “generally achieved” does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, “generally not achieved” indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of “generally not achieved” may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated “no assessment made.”

Table 31 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of critical infrastructure and key resources protection and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation’s key elements (generally not achieved).

Table 31: Performance Expectations and Assessment of DHS Progress in Critical Infrastructure and Key Resources Protection

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Develop a comprehensive national plan for critical infrastructure protection | *GAO findings:* DHS issued the National Infrastructure Protection Plan in June 2006. In October 2006, we reported that the National Infrastructure Protection Plan serves 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. We reported that each of the 17 critical infrastructure sectors had provided a sector-specific plan to DHS by the end of December 2006. In May 2007, DHS announced the completion of the 17 sector-specific plans. For more information see *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics,* GAO-07-39; *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure,* GAO-06-91; and *Homeland Security: Much Is Being Done to Protect Agriculture from a Terrorist Attack, but Important Challenges Remain,* GAO-05-214.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to develop a comprehensive national plan for critical infrastructure protection. DHS reported that each sector submitted by July 14, 2006, its sector Critical Infrastructure and Key Resources Protection Annual Report to DHS in which the sectors identified priorities and goals for critical infrastructure and key resources protection based on risk, need, and projected resource requirements. DHS also reported that on October 15, 2006, it finalized the National Critical Infrastructure and Key Resources Protection Annual Report, which is an aggregate of the sector annual reports.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation as DHS issued the National Infrastructure Protection Plan, which provides a comprehensive national plan for critical infrastructure protection. | Generally achieved |
| 2. Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector | *GAO findings:* DHS has taken steps to develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector. DHS is responsible for coordinating a national protection strategy, including formation of government and private sector councils as a collaborating tool. The councils, among other things, are to identify their most critical assets and identify protective measures in sector-specific plans that comply with DHS's National Infrastructure Protection Plan. In October 2006 we reported that all 17 critical infrastructure sectors established their respective government councils, and nearly all sectors initiated their voluntary private sector councils in response to the National Infrastructure Protection Plan. In addition, DHS has undertaken numerous initiatives to foster partnerships with other federal agencies, state and local governments, and the private sector about cyber attacks, threats, and vulnerabilities. For example, the National Cyber Response and Coordination Group facilitates coordination of intragovernmental and public/private preparedness and operations in order to respond to and recover from incidents that have significant cyber consequences and also brings together officials from national security, law enforcement, defense, intelligence, and other government agencies that maintain significant cybersecurity responsibilities and capabilities. For more information see GAO-07-39; *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity,* GAO-06-1087T; *Homeland Security: DHS Is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority Is Needed,* GAO-06-150; *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity,* GAO-05-827T; *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities,* GAO-05-434; and *Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges,* GAO-05-327.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to develop partnerships and coordinate with other federal agencies, state and | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | local governments, and the private sector. For example, DHS reported that its Protective Security Advisor program has provided support to state and local officials during incidents and contingencies and has made over 13,000 liaison visits to local jurisdictions and facilities and also established over 31,000 points of contact. DHS also reported that its Nuclear and Chemical Sector-Specific Agencies have cultivated relationships with their respective Government Coordinating Councils and Sector Coordinating Councils. DHS identified a number of other efforts these Sector-Specific agencies made. For example, the Chemical Sector-Specific Agency hosts biweekly Chemical Security teleconferences for senior chemical industry security managers. It also sponsors classified briefings for industry representatives and holds Government Coordinating Council meetings to discuss initiatives throughout the government that affect the chemical sector. Similarly, the Nuclear Sector-Specific Agency reported that it provides quarterly classified threat briefs by the Homeland Infrastructure Threat and Risk Analysis Center to the sector. It has also signed a memorandum of understanding with the Nuclear Sector Coordinating Council concerning the management and maintenance of the Homeland Security Information Network-Nuclear Sector and standard operating procedures agreements with the Nuclear Energy Institute and Constellation Energy for the safeguard and protection of classified information. The Emergency Service Sector Sector-Specific Agency reported that it uses the Emergency Services Regional Assessment Process to gather and analyze information provided by state, local, and tribal communities to identify capability weaknesses and protective measures for reducing or eliminating them.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has undertaken a number of efforts to develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector, such as coordinating collaborative tools detailed in the National Infrastructure Protection Plan. | |
| 3. Improve and enhance public/private information sharing involving attacks, threats, and vulnerabilities | *GAO and DHS IG findings:* While DHS has worked to improve and enhance public/private information sharing involving attacks, threats, and vulnerabilities, a number of challenges remain. In 2004, DHS piloted the Homeland Security Information Network, which is DHS's primary conduit through which it shares information on domestic terrorist threats, suspicious activity reports, and incident management. We reported in March 2006 that the Homeland Security Information Network platform for critical sectors was being developed and offered to each sector to provide a suite of information and communication tools to share critical information within the sector, with DHS, and eventually across sectors. However, in June 2006, the DHS IG reported that DHS had failed to take a number of key steps in planning and implementing the Homeland Security Information Network. For example, DHS did not provide adequate user guidance and had not developed specific performance measures for tracking information sharing on the Homeland Security Information Network. The DHS IG reported that as a result the Homeland Security Information Network was not effectively supporting state and local information sharing. In April 2007, we reported that DHS did not fully adhere to key practices in coordinating efforts on its Homeland Security Information Network with key state and local information-sharing initiatives. For example, it did not work with the two key state and local information-sharing initiatives (of the Regional Information Sharing System program) to fully develop joint strategies to meet mutual needs. It also did not develop compatible policies, procedures, and other means to operate across organizational boundaries. DHS's limited use of these practices is attributable in part to the department's expediting its schedule to deploy information-sharing capabilities after September 11, 2001, and in doing so not developing an inventory of key state and local information-sharing initiatives. We also reported that DHS officials have efforts planned and under way to improve coordination and collaboration, including establishing an advisory committee to obtain state and local views on network operations. DHS also plans to coordinate its efforts with the Administration's Information Sharing Environment initiative that aims to improve information sharing among all levels of government and the private sector. However, these activities have either just begun or are being planned. Consequently, until DHS develops an inventory of key state and local initiatives | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | and fully implements coordination and collaboration practices, it is at risk that effective information sharing is not occurring and that its Homeland Security Information Network may be duplicating state and local capabilities. This also raises the issue of whether similar coordination and duplication issues exist with the other homeland security networks, systems, and applications under DHS's purview.<br>In April 2006 we reported that DHS had issued an interim rule that established operating procedures for the receipt, care, and storage of critical infrastructure information, such as vulnerability assessments and security methods, and the agency has created a program office to administer the protected critical infrastructure information program. However, we noted that DHS had not defined the specific information—such as industry-specific vulnerabilities and interdependencies—needed under the program, nor has it comprehensively worked with other federal agencies with critical infrastructure responsibilities to find out what they need.<br>With regard to one critical infrastructure sector, the DHS IG reported in February 2007 that the National Infrastructure Coordinating Center, the Homeland Security Information Network Food and Agriculture portal, the Homeland Infrastructure Threat and Risk Analysis Center, and the Protected Critical Infrastructure Information program each had shortcomings concerning food sector information sharing. For example, the DHS IG reported that food sector experts expressed concern that while the Homeland Security Information Network Food and Agriculture portal had potential value, it had limited utility for the sector's information sharing purposes in its current form. For more information, see *Information Technology: Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives,* GAO-07-822T; *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives,* GAO-07-455; GAO-06-1087T; *Securing Wastewater Facilities: Utilities Have Made Important Upgrades but Further Improvements to Key System Components May Be Limited by Costs and Other Constraints*; GAO-06-390; *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information,* GAO-06-385; *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information,* GAO-06-383; GAO-06-150; GAO-05-434; *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors,* GAO-04-699T; and *Technology Assessment: Cybersecurity for Critical Infrastructure Protection,* GAO-04-321. Also, see Department of Homeland Security Office of Inspector General, *Homeland Security Information Network Could Support Information Sharing More Effectively,* OIG-06-38 (Washington, D.C.: June 2006) and *The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection,* OIG-07-33 (Washington, D.C.: February 2007).<br>*DHS updated information:* In March, April, and June 2007, DHS provided updated information regarding its efforts to improve and enhance public/private information sharing involving attacks, threats, and vulnerabilities. DHS reported that its Critical Infrastructure and Key Resources Information Sharing Environment encompasses a number of mechanisms that facilitate the flow of information, mitigate obstacles to voluntary information sharing by Critical Infrastructure and Key Resources owners and operators, and provide feedback and continuous improvement for structures and processes. DHS stated that the creation of an effective and efficient information sharing environment encompasses five components: governance (the sector partnerships), content, delivery vehicle (the Homeland Security Information Network and the National Infrastructure Coordination Center), relationship management, and an adaptive legal and policy framework to address the unique requirements of the critical infrastructure/key resources sectors. DHS stated the Homeland Security Information Network is a key enabler for information delivery. For example, in September 2006 testimony before the House Committee on Homeland Security, the Director of the Office of Operations Coordination stated that the Homeland Security Information Network "is the | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | primary, secure nationwide network through which DHS receives and shares critical information, including alerts and warnings, with its components and its public- and private-sector partners, including Federal, State, local, and tribal officials and the owners and operators of critical infrastructures". Yet DHS reported that the Homeland Security Information Network represents only one of the parts of the whole.<br><br>With regard to other elements of information sharing, DHS stated that it has developed its critical infrastructure/key resources information sharing environment strategy paper, a roadmap that describes and provides the basis for developing process and outcome metrics. DHS stated that this strategy has been accepted by the information sharing environment program manager as the way ahead for sharing information with the critical infrastructure/key resources sectors. DHS reported that within this framework, a critical infrastructure partnership advisory council working group has been established between the information sharing environment program manager and the private sector so the private sector can have direct representation in the decision making process regarding public/private information sharing. The department also reported that it had made a number of efforts to address concerns about the Homeland Security Information Network. For example, DHS stated that it is coordinating the implementation of the Homeland Security Information Network in state and local fusion centers and is implementing the DHS Common Operating Picture, which is a Web-based tool available through the Homeland Security Information Network that is designed to provide a common view of critical information to senior executive officials and other partners during a crisis. DHS also reported that it is focusing training and outreach efforts on state and local government throughout the Gulf Coast and East Coast regions, which the department sees as areas of high priority for hurricane season that would rely heavily on the Common Operating Picture and Homeland Security Information Network during incident response. Further, DHS stated that the National Infrastructure Coordination Center, which was established to maintain operational awareness of the nation's critical infrastructures and key resources, and provide a process and mechanism for information sharing and coordination with government and industry partners, has established processes to share routine and incident-driven information with sectors via the Homeland Security Information Network. DHS reported that the National Infrastructure Coordination Center also serves as the recognized DHS hub for critical infrastructure and key resources information during major incidents, facilitating daily interactive teleconferences with sector stakeholders; collecting, logging, and tracking information requests from critical infrastructure and key resources owners and operators; and providing a situation summary for stakeholders through the Common Operating Picture. DHS also stated that the National Infrastructure Protection Plan provided a framework for developing metrics for information sharing and that these metrics are in the process of being developed.<br><br>Further, DHS reported that its Technical Resource for Incident Prevention system—DHS's online, collaborative, information sharing network for bomb squad, law enforcement, and emergency services personnel to learn about current terrorist improvised explosive device tactics, techniques, and procedures—improves and enhances information sharing involving improvised explosive device attacks and threats. DHS also reported that in fiscal year 2007 it has had provided easier access to its Characteristics and Common Vulnerabilities, Potential Indicators of Terrorist Attack, and Protective Measure papers, which are derived from vulnerability assessments. DHS stated that in the past 6 months it has provide over 385 federal, state, local, and private sector stakeholders access to these reports through a web-based portal and that they are available on the Homeland Security Information Network.<br><br>DHS provided several examples of information sharing by the Nuclear Sector-Specific Agency, the Dams Sector-Specific Agency, the Emergency Sector-Specific Agency, and the Chemical Sector-Specific Agency. For example, DHS reported that every two weeks the Chemical Sector-Specific Agency hosts a security briefing teleconference for the chemical sector and twice a year will sponsor a classified briefing for all clear industry representatives. In addition, the Coast Guard reported that it launched Homeport in October 2005. The Coast Guard stated | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | that Homeport is an internet portal and the official Coast Guard information technology system for maritime security. The Coast Guard reported that Homeport provides instant access to information necessary to support increased information sharing requirements among federal, state, local and industry decision makers for security management and increased maritime domain awareness and is publicly accessible, providing all users with current maritime security information including DHS and Federal Bureau of Investigation threat products.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS identified five components to its information sharing environment—governance (the sector partnerships), content, delivery vehicle (the Homeland Security Information Network and the National Infrastructure Coordination Center), relationship management, and an adaptive legal and policy framework. According to the department, the Homeland Security Information Network is a key part of its information sharing efforts and serves as the primary mechanism for delivering information to its critical infrastructure partners. For example, in September 2006 testimony before the House Committee on Homeland Security, the Director of the Office of Operations Coordination stated that the Homeland Security Information Network "is the primary, secure nationwide network through which DHS receives and shares critical information, including alerts and warnings, with its components and its public- and private-sector partners, including Federal, State, local, and tribal officials and the owners and operators of critical infrastructures". In previous work, we and the DHS IG identified a number of challenges to the Homeland Security Information Network, such as coordination with state and local information sharing initiatives, and DHS did not provide evidence demonstrating that it has addressed these challenges. Further, in previous work, we also identified challenges to DHS's efforts to collect, care for, and store critical infrastructure information through its protected critical infrastructure information program. For example, DHS had not defined the specific information it needed nor had it worked with other federal agencies to find out what they needed. DHS also was not able to provide metrics indicating that its efforts have improved information sharing. As a result, it is difficult for Congress, us, and other stakeholders to assess the extent to which DHS's various initiatives have enhanced and improved information sharing related to critical infrastructure and key resources protection | |
| 4. Develop and enhance national analysis and warning capabilities for critical infrastructure | *GAO and DHS IG findings:* DHS has taken steps to develop and enhance national analysis and warning capabilities for critical infrastructure, but more work remains. Our work to date has primarily focused on cyber critical infrastructure protection and the DHS IG's work on the food and agriculture sector. In the cyber area, in May 2005 we reported that DHS has collaborated on, developed, and worked to enhance tools and communication mechanisms for providing analysis and warning of occurring and potential cyber incidents. Through its involvement in the U.S. Computer Emergency Readiness Team, DHS provides cyber analysis and warning capabilities by providing continuous operational support in monitoring the status of systems and networks. When a new vulnerability or exploit is identified, the U.S. Computer Emergency Readiness Team evaluates its severity, determines what actions should be taken and what message should be disseminated, and provides information through the National Cyber Security Division's multiple communications channels. However, we reported that DHS faced the same challenges in developing strategic analysis and warning capabilities that we reported on 4 years prior during a review of the National Cyber Security Division's predecessor. At that time, we reported that a generally accepted methodology for analyzing strategic cyber-based threats did not exist. We also reported that the center did not have the industry-specific data on factors such as critical systems components, known vulnerabilities, and interdependencies. In February 2007, the DHS IG reported that while DHS is not the designated lead for a number of key activities for food defense and critical infrastructure, Congress and the President have assigned DHS many important responsibilities in this area. The DHS IG identified several limitations in these efforts. For example, the DHS IG stated that modeling and simulation of food contamination incidents has not developed to the extent | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
|  | desirable. The DHS IG reported that DHS currently funds modeling and simulation efforts of the Critical Infrastructure Protection Decision Support System, the National Infrastructure Simulation and Analysis Center, and the National Center for Food Protection and Defense and that these programs have developed promising models in several areas of the food supply chain. The DHS IG reported that at the time of its fieldwork, these DHS-sponsored programs had developed detailed models or contamination scenarios for only the beef, dairy, corn, and fresh vegetable supply chains. The DHS IG also stated that experts in all three of the programs acknowledged that their models for these supply chains needed further refinement and could not account for the second- and third-order impacts of a major food contamination incident. For more information see GAO-06-383 and GAO-05-434. Also see Department of Homeland Security Office of Inspector General, *The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection,* OIG-07-33 (Washington, D.C.: February 2007).<br>*DHS updated information:* In March, April, and June 2007, DHS provided updated information regarding its efforts to develop and enhance national analysis and warning capabilities for critical infrastructure. DHS reported that over the past 2 years it has built out and continues to build the Critical Infrastructure Warning Information Network. DHS stated that the Critical infrastructure Warning Information Network is its critical, survivable network that connects DHS with the vital sector entities (including federal, state, private sector, and Canada and the United Kingdom) that are essential for restoring the nation's infrastructure during incidents of national significance. DHS stated that the Critical Infrastructure Warning Information Network has 143 Critical Infrastructure Warning Information Network members and provides both data and voice connectivity to allow its membership to exchange information, including alerts and notifications, as well as other routine information. DHS reported that it includes representation from all the critical infrastructure sectors, including 68 private sector entities that own and operate key concerns in the infrastructure sectors, as well as federal entities involved in monitoring and protecting them. DHS also reported that the Critical Infrastructure Warning Information Network connects the emergency operations centers of the 50 states and the District of Columbia to the DHS National Operations Center and is also used to provide classified connectivity and secure video teleconferencing between DHS and the states. Further, DHS stated that DHS's Office of Infrastructure Protection has sponsored a prompt notification pilot program with the Nuclear Sector Coordination Counsel. DHS reported that the pilot program demonstrated, for example, that DHS has the ability to ensure that nuclear sector infrastructure is promptly notified if infrastructure other than nuclear assets comes under attack nearby and that DHS can make notifications across its components, as well as to senior officials.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. While DHS has undertaken a number of efforts to develop and enhance national analysis and warning capacities for critical infrastructure, our prior work has shown that the department still faces a number of challenges. In the area of cybersecurity, for example, issues concerning methodology and data continue to pose challenges while a lack of collaboration creates challenges for its information gathering and/or analysis centers. These methodological issues in the cyber sector raise concerns as to whether sound methodologies exist for conducting analysis and warning in the other areas. Further, while DHS reported that it has expanded the Critical Infrastructure Warning Information Network, the department did not provide evidence demonstrating that it has enhanced national warning capabilities. |  |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 5. Provide and coordinate incident response and recovery planning efforts for critical infrastructure | *GAO and DHS IG findings:* DHS has faced challenges in its efforts to provide and coordinate incident response and recovery planning efforts in cases when critical infrastructure and key resources are attacked or otherwise affected by catastrophic events or disasters. Our work to date has primarily focused on cyber critical infrastructure protection. In that area, we reported in June 2006 that DHS had begun a variety of initiatives to fulfill its responsibility for developing an integrated public/private plan for Internet recovery, but these efforts were not yet complete or comprehensive. Specifically, DHS developed high-level plans for infrastructure protection and incident response, but the components of these plans that address the Internet infrastructure were not yet complete. We noted that key challenges to establishing a plan for recovering from an Internet disruption included (1) innate characteristics of the Internet (such as the diffuse control of the many networks that make up the Internet and the private sector ownership of core components) that make planning for and responding to disruptions difficult, (2) lack of consensus on DHS's role and when the department should get involved in responding to a disruption, (3) legal issues affecting DHS's ability to provide assistance to entities working to restore Internet service, (4) reluctance of many in the private sector to share information on Internet disruptions with DHS, and (5) leadership and organizational uncertainties within DHS. We reported that until these challenges were addressed, DHS would have difficulty achieving results in its role as a focal point for helping to recover the Internet from a major disruption. In September 2006, we reported that the nation's experience with Hurricane Katrina demonstrated that enhanced capabilities for catastrophic response and recovery were needed, particularly for capabilities such as the assessment of the disaster's effects, and communications. We noted that DHS had reported taking some actions to improve capabilities in response to findings in Congress' and the administration's reviews. However, ongoing work was still needed by DHS to address significant human resource challenges. In February 2007 the DHS IG reported that food contamination exercises provide key learning opportunities for food sector representatives, and generate valuable lessons about how the response to a food-related incident is likely to proceed and that Sector Coordinating Council and Government Coordinating Council representatives said that they found food contamination exercises to be very instructive. The DHS IG reported that DHS has provided little direct support for or attention to exercises relating to food contamination. Since 2003, DHS has provided direct support for only four post-harvest food-related exercises through Grants and Training's Exercise and Training Division. DHS has sponsored six additional post-harvest food contamination tabletop exercises through the Multi-State Partnership for Security in Agriculture. And while the June 1, 2006, National Exercise Schedule listed a total of 226 exercises over the following year, it did not register a single post-harvest food-related exercise. For more information see *Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System,* GAO-06-618; *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan,* GAO-06-672; GAO-05-434; and GAO-05-214. Also see Department of Homeland Security Office of Inspector General, *The Department of Homeland Security's Role in Food Defense and Critical Infrastructure Protection,* OIG-07-33 (Washington, D.C.: February 2007).<br>*DHS updated information:* In June 2007, DHS provided updated information regarding its efforts to provide and coordinate incident response and recovery planning efforts for critical infrastructure. DHS reported that it has led a coordinated effort with the Nuclear Regulatory Commission, the Environmental Protection Agency, the Department of Health and Human Services, the Department of Energy, and the Occupational Safety and Health Administration to develop interim Protective Action Guides for Radiological Dispersal Devices and Improvised Nuclear Device Incidents. DHS stated that the objective of the proposed guidance is to provide federal, state, local, and tribal decision-makers with uniform federal guidance to protect the public, emergency responders, and surrounding environments from the effects of radiation following an radiological dispersal devices or improvised nuclear device incident and to ensure that local and federal first responders can address any issues or circumstances that may arise. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
|  | DHS reported that use of this guidance in subsequent exercises has significantly improved the federal and state governments' ability to provide sound guidance to the public. DHS also reported that the Pandemic Flu Planning initiative for the Nuclear Sector is sponsored by the Nuclear Sector Coordination Council, in cooperation with DHS.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. While DHS has taken steps to provide and coordinate incident response and recovery planning efforts for critical infrastructure, our previous work has shown that DHS efforts to develop a public/private plan for Internet recovery were neither complete nor comprehensive. We also reported that a number of challenges existed that make it difficult to develop a plan. Further, in reviewing the nation's experience with Hurricane Katrina, we reported that enhanced capabilities for catastrophic response and recovery were needed. |  |
| 6. Identify and assess threats and vulnerabilities for critical infrastructure | *GAO and DHS IG findings:* DHS has identified and assessed threats and vulnerabilities for critical infrastructure. In December 2005 we reported that DHS has taken steps to identify and assess threats and vulnerabilities by, for example, establishing the National Asset Database, an inventory of approximately 80,000 assets, and developing and analyzing various threat scenarios. We also reported that DHS had begun work to develop threat scenarios and analyze them. We found that the Homeland Infrastructure Threat and Risk Analysis Center, staffed by sector specialists and intelligence analysts with backgrounds from the intelligence community, was responsible for generating these plausible threat scenarios and had developed 16, such as a suicide bomber and a weapon of mass destruction. However, DHS has faced challenges in, among other things, developing a way to differentiate the relative probability of various threats and a strategy for identifying, prioritizing, and coordinating the protection of critical infrastructure. In June 2006, the DHS IG reported that DHS was still in the process of identifying and collecting critical infrastructure and key resources data for populating the National Asset Database while also building the next version of it. The DHS IG also found that the National Asset Database contained numerous assets whose criticality was not obvious and found inconsistencies in what critical infrastructure and key resources states reported. Further, the DHS IG reported that the National Asset Database was not yet comprehensive enough to support the role envisioned for it in the National Infrastructure Protection Plan. In February 2007 we reported that DHS developed a method to estimate the relative risk of terrorist attacks to urban areas for the Urban Areas Security Initiative, a discretionary grant under the Homeland Security Grant Program. In fiscal year 2006, DHS estimated the risk faced by urban areas by assessing the relative risk of terrorism as a product of three components—threat, or the likelihood that a type of attack might be attempted; vulnerability, or the likelihood of a successful attack using a particular attack scenario; and consequence, or the potential impact of a particular attack. To estimate the relative risk, DHS assessed risk from two perspectives, asset-based and geographic, and then combined the assessments. To estimate asset risk, DHS computed the product of threat, vulnerability, and consequence by assessing the intent and capabilities of an adversary to successfully attack an asset type, such as a chemical plant, dam, or commercial airport, using one of 14 different attack scenarios. Simultaneously, 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. For fiscal year 2007, DHS officials stated that they will to continue to use the risk assessments to inform final funding decisions. They also described changes that simplified the risk methodology, integrating 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. While DHS stated that the department had made significant progress in developing its risk assessment methods, DHS officials told us that for the 2006 risk assessment process the department 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. For more information see | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | *Homeland Security Grants: Observations on Process DHS Used to Allocate Funds to Selected Urban Areas,* GAO-07-381R; GAO-06-91; and GAO-05-434. Also, see Department of Homeland Security Office of Inspector General, *Progress in Developing the National Asset Database,* OIG-06-40 (Washington, D.C.: June 2006).<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to identify and assess threats and vulnerabilities for critical infrastructure. For example, DHS has conducted over 2,600 vulnerability assessments on every critical infrastructure sector though the Comprehensive Review program, the Buffer Zone Protection Program, and the Site Assistance Visit program. DHS describes the Comprehensive Review as a structured, collaborative government and private sector analysis of high value critical infrastructure and key resources facilities. The purpose of the review is to explore exposure to potential terrorist attacks, their consequences, and the integrated prevention and response capabilities of stakeholders.<br>Through the Buffer Zone Protection Program, and with the support of DHS, local authorities develop Buffer Zone Protection Plans, which DHS reported have several purposes, including identifying specific threats and vulnerabilities associated with the buffer zone and analyzing the level of risk associated with each vulnerability. DHS describes the Site Assistance Visit Program as an information gathering visit with several goals, such as better understanding and prioritizing vulnerabilities of critical infrastructure and key resources and increasing awareness of threats and vulnerabilities among critical infrastructure and key resources owners and operators. DHS has conducted a total of 49 Comprehensive Reviews, 1,900 Buffer Zone Plans, and 700 Site Assistance Visits and reported that more are scheduled throughout fiscal year 2007.<br>The Coast Guard stated that it is a partner in the Comprehensive Review process and reported that the results of the Comprehensive Reviews and Port Security Assessments were entered into the Maritime Security Risk Analysis Model to prioritize risk according to a combination of possible threat, consequence, and vulnerability scenarios. The Coast Guard stated that under this approach, seaport infrastructure that was determined to be both a critical asset and a likely and vulnerable target would be a high priority for funding security enhancements while infrastructure that was vulnerable to attack but not as critical or that was very critical but already well-protected would be lower in priority. Further, DHS reported that through its Strategic Homeland Infrastructure Risk Assessment program, the Homeland Infrastructure Threat and Risk Analysis Center has developed a methodology for comparing and prioritizing risks across infrastructure sectors. According to DHS, the Center differentiates the relative probability of various threats. DHS stated that the Strategic Homeland Infrastructure Risk Assessment was produced in 2006 and it served as the National Critical Infrastructure and Key Resources Risk Profile in the 2006 National Critical Infrastructure and Key Resources Protection Annual Report. DHS reported that this risk assessment model provides a mechanism to capture threat estimates based on terrorist capability and the intent to attach critical infrastructure and key resources. The Homeland Infrastructure Threat and Risk Analysis Center provides sources for all analytical judgments and coordinates the threat analysis with the Intelligence Community. These estimates provide the basis for differentiating the relative probability of the threat for each scenario assessed in the Strategic Homeland Infrastructure Risk Assessment report. DHS also reported that the department uses information contained within the National Asset Database, further informed by comprehensive risk analysis, to facilitate prioritization of the support it provides to help secure the nation's infrastructure. DHS stated that in collaboration with the Sector-Specific Agencies and state governments, it has developed a list of the nation's most important infrastructure to assets to inform the 2007 grants program. DHS stated that this prioritization allows it to focus its planning, stakeholder interaction, and resource allocation on those sites with the potential to have a severe impact on public health, governance, the economy, or national security. | |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | *Our assessment:* We conclude that DHS has generally achieved this performance expectation, as DHS has taken a number of steps to identify and assess threats and vulnerabilities for critical infrastructure. For example, DHS has conducted over 2,600 vulnerability assessments on each of the 17 critical infrastructure sectors, and it has conducted a total of 49 Comprehensive Reviews, 1,900 Buffer Zone Plans, and 700 Site Assistance Visits and reported that more are scheduled throughout fiscal year 2007. DHS has also assessed threats and vulnerabilities through its risk estimates for the Urban Areas Security Initiative. | |
| 7. Support efforts to reduce threats and vulnerabilities for critical infrastructure | *GAO findings:* DHS has supported efforts to reduce threats and vulnerabilities for critical infrastructure. Supporting efforts have included targeted infrastructure protection grants, research and development, and sharing best practices. DHS has funded research in different critical infrastructure areas. In 2005, DHS released a national research and development plan supporting critical infrastructure protection, but acknowledged at the time, though, that it was a baseline plan and did not include an investment plan and road map that were to be added in 2006. In July 2005 we reported that in the area of cybersecurity DHS had initiated efforts to reduce threats by enhancing collaboration with the law enforcement community and to reduce vulnerabilities by shoring up guidance on software and system security. However, we reported that efforts were not completed and that vulnerability reduction efforts were limited until the cyber-related vulnerability assessments were completed. In February 2007 we reported that in fiscal year 2006, DHS provided approximately $1.7 billion in federal funding to states, localities, and territories through its Homeland Security Grant Program to prevent, protect against, respond to, and recover from acts of terrorism or other catastrophic events. In fiscal year 2006, DHS awarded approximately $711 million in Urban Areas Security Initiative grants, discretionary grants under the Homeland Security Grant Program—a 14 percent reduction in funds from the previous year—while the number of eligible urban areas identified by the risk assessment decreased from 43 to 35. In March 2007 we reported that DHS had used various programs to fund passenger rail security since 2003. For example, the fiscal year 2005 DHS appropriations act provided $150 million for intercity passenger rail transit, freight rail, and transit security grants. DHS used this funding to create and administer new programs focused specifically on transportation security, including the Transit Security Grant Program and the Intercity Passenger Rail Security Grant Program, which provided financial assistance to address security preparedness and enhancements for passenger rail and transit systems. During fiscal year 2006, DHS provided $110 million to passenger rail transit agencies through the Transit Security Grant Program and about $7 million to Amtrak through the Intercity Passenger Rail Security Grant Program. While DHS has distributed hundreds of millions of dollars in grants to improve passenger rail security, issues have surfaced about the grant process. As DHS works to refine its risk assessment methodologies, develop better means of assessing proposed investments using grant funds, and align grant guidance with the implementation of broader emergency preparedness goals, such as implementation of the National Preparedness Goal, it has annually made changes to the guidance for the various grants it administers. As a result of these annual changes, awardees and potential grant recipients must annually review and understand new information on the requirements for grant applications, including justification of their proposed use of grant funds. Further, while funds awarded through the Transit Security Grant Program can be used to supplement funds received from other grant programs, allowable uses are not clearly defined. For more information see *Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts*, GAO-07-583T; GAO-07-381R; *Information Security: Coordination of Federal Cyber Security Research and Development,* GAO-06-811; GAO-05-827T; GAO-05-434; and *Homeland Security: Much Is Being Done to Protect Agriculture from a Terrorist Attack, but Important Challenges Remain*, GAO-05-214.<br>*DHS updated information*: In March, April, and June 2007 DHS provided us with updated information on its efforts to support efforts to reduce threats and vulnerabilities for critical infrastructure. Through the Buffer Zone Protection Program, DHS reported that it assists local | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
|  | law enforcement to make it more difficult for terrorists to conduct surveillance or successfully launch attacks from the immediate vicinity of critical infrastructure and key resources targets. DHS reported that in fiscal years 2005 and 2006 Buffer Zone Protection Program grants awarded to the states totaled approximately $140 million. DHS stated that the program requires that funding be subgranted to the responsible jurisdictions in support of prevention and protection focused activities. DHS stated that of the approximately $140 million awarded, the majority, approximately $107 million, or approximately 76 percent, has gone to law enforcement organizations as subgrantees. DHS reported that the remaining funding was subgranted to other disciplines, such as emergency management, agriculture, and cyber security, with emergency management receiving the second highest proportion of the funds, approximately $18 million or 13 percent. DHS also reported that it is documenting, through the Vulnerability Reduction Purchasing Plan, how sub-grantees are utilizing grant money to reduce threats and vulnerabilities based on the Buffer Zone Plan, Buffer Zone Protection Program guidance, and the Authorized Equipment list, a DHS reference tool. Further, in April 2007, DHS released the Chemical Facilities Anti-Terrorism Standards, which established risk-based performance standards for the security of chemical facilities. DHS provided several examples of how the Nuclear Sector-Specific Agency, the Dams Sector-Specific Agency, the Chemical Sector-Specific Agency, and the Commercial Facilities Sector-Specific Agency have supported efforts to reduce threats and vulnerabilities for critical infrastructure. For example, DHS reported that the Dams Sector-Specific Agency is supporting a study on the vulnerabilities of dams to terrorist attacks using large aircraft impact as the attack scenarios and that the Nuclear Sector-Specific Agency has established the Comprehensive Review Outcomes Working Network to reach back to the sites where Comprehensive Reviews were conducted, identify the status of the gaps and potential enhancements identified by the team, and continue the open and candid dialogue between the government, industry, and State/local emergency services organizations. In addition, DHS reported that the department's Office for Bombing Prevention conducts capabilities assessments of public safety bomb squads, explosives detection canine teams, and public safety dive teams.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has funded research in different critical infrastructure areas and, in the area of cybersecurity, initiated efforts to reduce threats by enhancing collaboration with the law enforcement community and to reduce vulnerabilities by shoring up guidance on software and system security. However, while DHS has taken steps to support efforts to reduce threats and vulnerabilities for critical infrastructure, our prior work has shown that challenges remain. For example, DHS has issued different targeted infrastructure protection grants, but allowable uses of some of these grants are not clearly defined. Further, DHS has released the Chemical Facilities Anti-Terrorism Standards, but it is too early to evaluate their impact. |  |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

## DHS Has Made Limited Progress in the Area of Science and Technology

DHS's Science and Technology Directorate was established to coordinate the federal government's civilian efforts to identify and develop countermeasures to chemical, biological, radiological, nuclear, and other emerging terrorist threats to our nation. To coordinate the national effort to protect the United States from nuclear and radiological threats, in April 2005, the President directed the establishment of the Domestic Nuclear Detection Office within DHS. The new office's mission covers a broad spectrum of responsibilities and activities, but is focused primarily on providing a single accountable organization to develop a layered defense system. This system is intended to integrate the federal government's nuclear detection, notification, and response systems. In addition, under the directive, the Domestic Nuclear Detection Office is to acquire, develop, and support the deployment of detection equipment in the United States, as well as to coordinate the nation's nuclear detection research and development efforts.

As shown in table 32, we identified six performance expectations for DHS in the area of science and technology, and we found that overall DHS has made limited progress in meeting those performance expectations. In particular, we found that DHS has generally achieved one performance expectation and has generally not achieved five other performance expectations.

Table 32: Performance Expectations and Progress Made in Science and Technology

| | Assessment | | |
|---|---|---|---|
| Performance expectation | Generally achieved | Generally not achieved | No assessment made |
| 1. Develop a plan for departmental research, development, testing, and evaluation activities | | ✓ | |
| 2. Assess emerging chemical, biological, radiological, and nuclear threats and homeland security vulnerabilities | | ✓ | |
| 3. Coordinate research, development, and testing efforts to identify and develop countermeasures to address chemical, biological, radiological, nuclear, and other emerging terrorist threats | | ✓ | |
| 4. Coordinate deployment of nuclear, biological, chemical, and radiological detection capabilities and other countermeasures | | ✓ | |
| 5. Assess and evaluate nuclear, biological, chemical, and radiological detection capabilities and other countermeasures | | ✓ | |
| 6. Coordinate with and share homeland security technologies with federal, state, local, and private sector entities | ✓ | | |
| **Total** | 1 | 5 | 0 |

Source: GAO analysis.

Note: An assessment of “generally achieved” indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of “generally achieved” does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, “generally not achieved” indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of “generally not achieved” may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated “no assessment made.”

Table 33 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of science and technology and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation’s key elements (generally not achieved).

Table 33: Performance Expectations and Assessment of DHS Progress in Science and Technology

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Develop a plan for departmental research, development, testing, and evaluation activities | *GAO and DHS IG findings:* DHS has not yet developed a plan for its research, development, testing, and evaluation activities to achieve this performance expectation. In 2004, we reported that DHS was still developing a strategic plan to identify priorities, goals, objectives, and policies for the research and development of countermeasures to nuclear, biological, chemical, and other emerging terrorist threats. We reported that completion of this strategic plan was delayed because much of the time since DHS's March 2003 creation had been spent organizing the Science and Technology Directorate, developing policies and procedures, and hiring necessary staff. In addition, the DHS IG has reported that the Science and Technology Directorate had to contend with a set of administrative and logistical challenges similar to those encountered by other startup ventures, including the inability to hire personnel quickly who can work in a secure environment, the lack of centralized space, and the lack of consistent information technology systems and procurement support. For more information, see *Homeland Security: DHS Needs to Improve Ethics-Related Management Controls for the Science and Technology Directorate,* GAO-06-206; *Transportation Security R&D: TSA and DHS Are Researching and Developing Technologies, but Need to Improve R&D Management,* GAO-04-890; and *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. Also, see Department of Homeland Security Office of Inspector General, *Survey of the Science and Technology Directorate,* OIG-04-24 (Washington, D.C.: March 2004).<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to develop a plan and strategy for research, development, testing, and evaluation activities. The department reported that it has put into place a combined organization and research portfolio strategy within the Science and Technology Directorate aimed at identifying and transitioning homeland security capabilities to customers. As part of these efforts, DHS developed its FY2007-2008 Science and Technology Execution Plan, which details the Science and Technology Directorate's research, development, testing, and evaluation activities planned for those years. The plan includes an overview of the mission, strategy, and function of each Science and Technology Directorate division. DHS has also developed and released its Technology Development and Transfer report, which provides information on the department's strategy and approach to homeland security research, development, testing, and evaluation. In June 2007, DHS released the Science and Technology Directorate Strategic Plan, which included the Science and Technology Directorate Five-Year Research and Development Plan (fiscal years 2007 through 2011).<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Since our prior work, DHS has developed plans and reports that, according to the department, reflect its overall strategy for research, development, testing, and evaluation activities. However, our assessment of these plans and reports shows that they do not include key elements of a strategic plan, such as goals, measures, and milestones. For example, the FY2007-2008 Science and Technology Execution Plan discusses activities for a 2-year period and does not include performance measures and goals for the department's research, development, testing, and evaluation activities. The report on Technology Development and Transfer provides a framework for how the Science and Technology Directorate plans to conduct its activities but does not define the work to be undertaken by the directorate. The Science and Technology Directorate Strategic Plan and associated Five-Year Research Development Plan provide information on deliverables and milestones for fiscal years 2007 through 2011. However, these plans do not include goals and measures for the department's science and technology activities. In addition, according to the department, these plans do not address the requirement in the Homeland Security Act of 2002 for the department to develop a national policy and strategic plan for identifying priorities, goals, | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | objectives, and policies for, and coordinating the federal government's civilian efforts to identify and develop countermeasures to chemical, biological, and other emerging terrorist threats, upon which this performance expectation is, in part, based. | |
| 2. Assess emerging chemical, biological, radiological, and nuclear threats and homeland security vulnerabilities | *GAO findings:* In 2004, we reported that DHS was in the process of conducting risk assessments of various critical infrastructure sectors. We reported that in the absence of completed risk assessments, DHS officials were using available threat intelligence, expert judgment, congressional mandates, mission needs, and information about past terrorist incidents to select and prioritize their research and development projects. For more information, see GAO-04-890.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to assess emerging chemical, biological, radiological, and nuclear threats and homeland security vulnerabilities. In fiscal year 2006, DHS completed and distributed the Bioterrorism Threat Risk Assessment that calculates risk for 28 biological threats agents considered in the context of numerous possible scenarios, including aerosol dissemination and food and water contamination. According to DHS, the process used for determining bioterrorism risks included estimating the probabilities of occurrence for the scenarios under consideration and then calculating consequences for those scenarios should they occur. DHS reported that the Bioterrorism Threat Risk Assessment has been used as a basis for other assessments, the definition of intelligence collection requirements, and technology development and to help decision makers evaluate possible risk mitigation strategies. The Science and Technology Directorate is currently updating this assessment to include agricultural and economic effects and plans to reissue it in fiscal year 2008. DHS reported that it is currently conducting a Chemical Threat Risk Assessment and the Integrated Chemical, Biological, Radiological, and Nuclear Assessment to be delivered in June 2008. DHS is also conducting four chemical threat assessments, and these threat assessments are known as Population Threat Assessments. Each Population Threat Assessment depicts a plausible, high-consequence scenario and addresses aspects of an attack process, including the possible acquisition, production, and dissemination of agents that could result in a high consequence event. The assessment then provides an estimate of the number of people potentially exposed to different doses of the threat. The Population Threat Assessments are intended to assess potential human exposures from a chemical, biological, radiological, or nuclear event and provide population exposure estimates to perform consequence modeling studies. Moreover, according to DHS, the Biodefense Knowledge Center and the Chemical Security Analysis Center assess known and emerging threats and issue Technical Bulletins on threats and vulnerabilities.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has completed some assessments on biological and chemical threats and vulnerabilities. However, DHS is still in the process of completing assessments in the chemical sector as well as its Integrated Chemical, Biological, Radiological, and Nuclear Assessment. Although DHS plans to take actions to assess threats and vulnerabilities over time, including updating past assessments, DHS's assessment efforts overall appear to be the early stages, and substantial more work remains for DHS to more fully conduct assessments of chemical, biological, radiological, and nuclear threats. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 3. Coordinate research, development, and testing efforts to identify and develop countermeasures to address chemical, biological, radiological, nuclear, and other emerging terrorist threats | *GAO findings:* In prior work we reported that with the creation of the Domestic Nuclear Detection Office in April 2005, DHS took an important step in coordinating national research efforts to address emerging threats. Among other responsibilities, the Domestic Nuclear Detection Office is taking the lead in developing a "global architecture," an integrated approach to detecting and stopping nuclear smuggling. However, we reported that because the Domestic Nuclear Detection Office was created so recently, these efforts are in their early stages of development and implementation. With regard to radiation portal monitors, in March 2006 we reported that DHS has sponsored research, development, and testing activities that attempt to improve the capabilities of existing radiation portal monitors and to produce new, advanced technologies with even greater detection and identification enhancements. However, we noted that much work remained for the agency to achieve consistently better detection capabilities. For example, DHS sponsored the development of a software package designed to reduce the number of false alarms from portal monitors already in widespread use. Further, we found that DHS was testing advanced portal monitors that use a technology designed to both detect the presence of radiation and identify its source. In addition, we reported that DHS has sponsored a long-range research program aimed at developing innovative technologies designed to improve the capabilities of radiation detection equipment. More recently, in October 2006 we reported that the Domestic Nuclear Detection Office's cost-benefit analysis for the acquisition and deployment of new portal monitors did not provide a sound analytical basis for the office's decision to purchase and deploy new portal monitor technology. Specifically, we reported that the Domestic Nuclear Detection Office did not use the results of its own performance tests in its cost-benefit analysis and instead relied on assumptions of the new technology's anticipated performance level. Furthermore, the analysis did not include the results from side-by-side tests that the Domestic Nuclear Detection Office conducted of the advanced portal monitors and current portal monitors. The cost-benefit analysis for acquiring and deploying portal monitors was also incomplete because it did not include all of the major costs and benefits required by DHS guidelines. In particular, the Domestic Nuclear Detection Office did not assess the likelihood that radiation detection equipment would either misidentify or fail to detect nuclear or radiological material. Rather, it focused its analysis on reducing the time necessary to screen traffic at border checkpoints and reduce the impact of any delays on commerce. In March 2007, we reported that the Domestic Nuclear Detection Office had not yet collected a comprehensive inventory of testing information on commercially available portal monitors. Such information—if collected and used—could improve the office's understanding of how well portal monitors detect different radiological and nuclear materials under varying conditions. In turn, this understanding would assist the Domestic Nuclear Detection Office's future testing, development, deployment, and purchases of portal monitors. We also reported that the Domestic Nuclear Detection Office has been improving its efforts to provide technical and operational information about radiation portal monitors to state and local authorities. For example, the office helped to establish a Web site that, among other things, includes information for state and local officials on radiation detection equipment products and performance requirements. However, some state representatives, particularly those from states with less experience conducting radiation detection programs, would like to see the Domestic Nuclear Detection Office provide more prescriptive advice on what types of radiation detection equipment to deploy and how to use it. For more information, see *Combating Nuclear Smuggling: DNDO Has Not Yet Collected Most of the National Laboratories' Test Results on Radiation Portal Monitors in Support of DNDO's Testing and Development Program,* GAO-07-347R; *Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports-of-Entry, but Concerns Remain,* GAO-06-389; *Combating Nuclear Smuggling: DHS's Cost-Benefit Analysis to Support the Purchase of New Radiation Detection Portal Monitors Was Not Based on Available Performance Data and Did Not Fully Evaluate All the Monitors' Costs and Benefits,* GAO-07-133R; and GAO-04-653. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | *DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to coordinate research, development, and testing efforts to identify and develop countermeasures to address threats. According to DHS, the Science and Technology Directorate is currently developing and testing several systems to provide the technology needed to counter the use of chemical and biological weapons. There are currently 6 projects under development as chemical countermeasures and 10 projects for biological counter measures. These countermeasures include sensors, detection capabilities, and identification systems. DHS also reported that the interagency Technical Support Working Group has worked with the DHS Science and Technology Directorate to identify technologies that could assist DHS customers in addressing their capability gaps. The DHS Science and Technology Directorate also noted that it has taken steps, such as establishing an International Program Division, to coordinate efforts with international partners. DHS also reported that it works with other federal agencies and entities to coordinate research and development activities, including the National Science and Technology Council's Committee on Homeland and National Security; the National Nuclear Security Administration; the Departments of Defense, Energy, Health and Human Services; the Food and Drug Administration; the Centers for Disease Control; and the Environmental Protection Agency. DHS reported that in 2004 it started four Regional Technology Integration pilots to test chemical and biological explosives detection systems; planning and exercise tools to evaluate performance; and technologies for credentialing emergency responders and verifying victims' identities during an incident.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has taken some actions to coordinate research, development, and testing efforts to identify and develop countermeasures to address various threats. Specifically, DHS has taken actions to develop and test various capabilities to detect the presence of radiation in cargo entering the United States. DHS has also coordinated research, development, and testing activities for detecting and identifying biological and chemical threats. However, DHS has not always comprehensively collected testing shared information with regard to radiation portal monitors, and some state officials have identified concerns in the advice on the monitors provided by DHS. Moreover, as previously discussed, DHS has completed some assessments of threats and vulnerabilities and is in the processing of conducting others. Until these assessments are completed across the nuclear, radiological, biological, and chemical sectors, DHS may not fully know what technologies or countermeasures and associated requirements are needed to address identified threats and vulnerabilities. | |
| 4. Coordinate deployment of nuclear, biological, chemical and radiological detection capabilities and other countermeasures | *GAO findings:* In prior work, we reported on the progress DHS has made in coordinating the deployment of capabilities for screening containerized shipments entering the United States. As of February 2006, CBP estimated that it had the ability to screen about 62 percent of all containerized shipments entering the United States and roughly 77 percent of all private vehicles. However, we reported that CBP and Pacific Northwest National Laboratory were behind schedule in deploying radiation portal monitors and would have to increase the speed of deployment by almost 230 percent in order to meet their September 2009 program completion date. For more information, see GAO-06-389 and GAO-04-890.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to coordinate the deployment of nuclear, biological, chemical, and radiological detection capabilities and countermeasures. For example, DHS reported as of March 2007, it was scanning 91 percent of containerized cargo entering the United States by land and sea for radiation, deploying 283 new portal monitors in fiscal year 2006 and bringing the total number of deployed portal monitors to 966 as of March 9, 2007. DHS has deployed the BioWatch system, a biological and chemical aerosol monitoring system, in more than 30 cities nationwide to provide early warning of a bio-attack. DHS also reported that it is piloting the Biological Warning and Incident Characterization system to better and more rapidly characterize the public health effects of a BioWatch positive indication. DHS also reported | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | that it has deployed the Rapidly Deployable Chemical Defense Systems to multiple national security special events. This system is a network of chemical ground-based detectors and aerial surveillance monitors that can identify specific chemical compounds and image the impact of a downwind chemical hazard. DHS has also deployed the Program for Response Options and Technology Enhancements for Chemical Terrorism that detects the release of toxic chemical agents in subway systems. In addition, through the Public Health Actionable Assays project, DHS is working to establish sampling evaluation and biodetection standards by developing a mechanism for rigorous, independent evaluation and validation of Assay Technologies.<br>*Our assessment:* We conclude that DHS has generally not yet achieved this performance expectation. DHS has taken actions to coordinate the deployment of various chemical, biological, radiological, and nuclear detection capabilities and countermeasures. In particular, DHS has deployed various systems to ports of entry, for example, to detect possible nuclear or radiological materials entering the United States. DHS has also deployed systems to detect the presence of biological or chemical agents in the air and to provide warning of the presence of these agents. However, DHS generally did not provide us with documentation on its efforts to coordinate the deployment of countermeasures beyond radiation detection capabilities at ports of entry and monitoring of possible aerosol-based attacks. Moreover, as previously discussed, DHS has completed some assessments of threats and vulnerabilities and is in the processing of conducting others. Until these assessments are completed across the nuclear, radiological, biological, and chemical sectors, DHS may not fully know what technologies or countermeasures and associated requirements are needed to address identified threats and vulnerabilities. Although we see progress in DHS's activities for deploying capabilities and countermeasures, much more work is needed for us to conclude that DHS has generally achieved this performance expectation. | |
| 5. Assess and evaluate nuclear, biological, chemical, and radiological detection capabilities and other countermeasures | *GAO findings:* In prior work we reported on the effort to test radiation detection equipment. We reported that in February 2005, DHS sponsored testing of commercially available portal monitors, isotope identifiers, and pagers against criteria set out in American National Standards Institute standards. These standards provided performance specifications and test methods for testing radiation detection equipment, including portal monitors and handheld devices. The actual testing was performed by four Department of Energy laboratories, with coordination, technical management, and data evaluation provided by the Department of Commerce's National Institute for Standards and Technology. The laboratories tested a total of 14 portal monitors from eight manufacturers against 29 performance requirements in the standards. Overall, none of the radiation detection equipment, including the portal monitors and handheld devices deployed by CBP, met all of the performance requirements in this first round of testing. However, according to Science and Technology Directorate officials, many of the limitations noted in CBP's equipment were related to withstanding environmental conditions—not radiation detection or isotope identification. More recently, in March 2007 we reported that the Domestic Nuclear Detection Office had not yet collected a comprehensive inventory of testing information on commercially available polyvinyl toluene portal monitors, which detect the presence of radiation but cannot distinguish between benign, naturally occurring radiological materials, such as ceramic tile, and dangerous materials, such as highly enriched uranium. We reported that such information—if collected and used—could improve the Domestic Nuclear Detection Office's understanding of how well portal monitors detect different radiological and nuclear materials under varying conditions. In turn, this understanding would assist the Domestic Nuclear Detection Office's future testing, development, deployment, and purchases of portal monitors. Radiation detection experts with the national laboratories and industry told us that, in their view, the Domestic Nuclear Detection Office should collect and maintain all the national laboratory test reports on commercially available portal monitors because these reports provide a comprehensive inventory of how well portal monitors detect a wide variety of radiological and nuclear | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | materials and how environmental conditions and other factors may affect performance. For more information, see GAO-07-347R and GAO-06-389.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to assess and evaluate nuclear, biological, chemical, and radiological detection capabilities and countermeasures. DHS reported that the Domestic Nuclear Detection Office has conducted a variety of tests on radiation portal monitors. In addition, DHS reported that the Domestic Nuclear Detection Office has worked with various partners to develop a global nuclear detection architecture that identifies vulnerabilities and is used by DHS and its partners as a basis for assessing gaps in detection capabilities and identifying possible paths from the original source of the radiological or nuclear material to targets within the United States. DHS also reported that it has evaluated the capabilities it has deployed to address chemical and biological threats, including BioWatch and Rapidly Deployable Chemical Detection Systems. In addition, DHS has participated in efforts to develop and assess a set of procedures, plans, and technologies to rapidly restore transportation nodes following a biological attack, with a focus on major international airports.<br>*Our assessment:* We conclude that DHS has generally not yet achieved this performance expectation. DHS has undertaken efforts to assess its chemical, biological, radiological, and nuclear detection capabilities, including radiation portal monitors and BioWatch. However, we identified concerns about DHS's efforts to collect and analyze data on the results of testing of radiation mortal monitors, and DHS did not provide us with evidence on the results of its efforts to assess countermeasures deployed to address chemical, biological, radiological, and nuclear threats. Although we see progress in DHS's activities for assessing deployed capabilities and countermeasures, much more work is needed for us to conclude that DHS has generally achieved this performance expectation. | |
| 6. Coordinate with and share homeland security technologies with federal, state, local, and private sector entities | *GAO and DHS IG findings:* DHS has taken actions to coordinate with homeland security partners. For example, DHS has coordinated with some interagency groups, including the National Security Council's Policy Coordinating Committee for Counterterrorism and National Preparedness. DHS also cochairs a standing committee on Homeland and National Security in the White House's Office of Science and Technology Policy. This committee identifies key areas requiring interagency coordination in the formulation of research and development agendas. DHS has also worked with the Technical Support Working Group—an interagency working group of representatives from over 80 federal agencies that is jointly overseen by the Departments of State and Defense. DHS also coordinated some of its research and development projects with other federal agencies. For example, DHS is responsible for BioWatch, a federal program that monitors about 30 major cities for chemical and biological threats. BioWatch is executed jointly by DHS, Department of Energy's laboratories, the Environmental Protection Agency, and the Centers for Disease Control and Prevention. In March 2007, we reported that with regard to radiation portal monitors, the Domestic Nuclear Detection Office has been improving its efforts to provide technical and operational information about radiation portal monitors to state and local authorities. For example, the Domestic Nuclear Detection Office recently helped to establish a Web site that, among other things, includes information for state and local officials on radiation detection equipment products and performance requirements. However, some state representatives with whom we spoke, particularly those from states with less experience conducting radiation detection programs, would like to see the Domestic Nuclear Detection Office provide more prescriptive advice on what types of radiation detection equipment to deploy and how to use it. For more information, see GAO-07-347R, GAO-04-653, and GAO-04-890.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to coordinate with and share homeland security technologies with federal, state, local, and private sector entities. For example, DHS reported that the Domestic Nuclear Detection Office has supported the Domestic Nuclear Defense Research and | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | Development Working Group to develop a coordinated research and development roadmap for domestic nuclear defense efforts. Specifically, this working group coordinates research and development strategies for domestic nuclear defense, the identification and filling of technology gaps, efforts to develop and sustain capabilities through appropriate investments in science and research, interagency funding for science and technology, and collaboration and exchange of research and development information. DHS reported that this working group's initial report was completed in January 2006 and that the roadmap is currently being updated, with a scheduled completion date of September 2007. The DHS Science and Technology Directorate reported that its Technology Clearinghouse and TechSolutions initiatives provide direct support to emergency responders. The Technology Clearinghouse is designed to provide access to technology information for federal, state, and local public safety and first responder entities. TechSolutions provides a Web-based mechanism for first responders to provide information on their capability gaps. The Science and Technology Directorate responds by identifying existing technology that could meet the need or, if no existing technology is available, to prototype a possible solution. DHS has also signed a memorandum of understanding with the Department of Health and Human Services, the Department of Defense, the Department of Justice, and the U.S. Postal Service for the coordination of air monitoring programs and, among other things, the development a national architecture and joint technology roadmap for investing in technologies for monitoring biological threats. Moreover, the Science and Technology Directorate has established centers for analysis and development efforts with other federal agencies. In addition, metropolitan subway systems have taken over operation of the Program for Response Options and Technology Enhancements for Chemical Terrorism, a system that detects releases of toxic chemical agents.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has taken actions to coordinate with and share homeland security technologies with a wide variety of partners. | |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

## DHS Has Made Modest Progress in Acquisition Management

Federal agencies use a variety of approaches and tools, including contracts, to acquire goods and services needed to fulfill or support the agencies' missions. DHS has some of the most extensive acquisition needs within the U.S. government. In fiscal year 2004, for example, the department obligated $9.8 billion to acquire a wide range of goods and services—such as information systems, new technologies, weapons, aircraft, ships, and professional services. In fiscal year 2006, the department reported that it obligated $15.6 billion to acquire a wide range of goods and services. The DHS acquisitions portfolio is broad and complex. For example, the department has purchased increasingly sophisticated screening equipment for air passenger security; acquired technologies to secure the nation's borders; purchased trailers to meet the housing needs of Hurricane Katrina victims; and is upgrading the Coast Guard's offshore fleet of surface and air assets. DHS has been working to integrate the many acquisition processes and systems that the disparate agencies and organizations brought with them when they merged into DHS in 2003 while still addressing ongoing mission requirements and emergency situations, such as responding to Hurricane Katrina.

As shown in table 34, we identified three performance expectations for DHS in the area of acquisition management and found that overall DHS has made modest progress in meeting those expectations. Specifically, we found that DHS has generally achieved one and not achieved two of the three performance expectations.

**Table 34: Performance Expectations and Progress Made in Acquisition Management**

| | Assessment | | |
|---|---|---|---|
| **Performance expectation** | **Generally achieved** | **Generally not achieved** | **No assessment made** |
| 1. Assess and organize acquisition functions to meet agency needs | ✓ | | |
| 2. Develop clear and transparent policies and processes for all acquisitions | | ✓ | |
| 3. Develop an acquisition workforce to implement and monitor acquisitions | | ✓ | |
| **Total** | **1** | **2** | **0** |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

Table 35 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of acquisition management and our assessment of whether DHS has taken steps to  satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation's key elements (generally not achieved).

**Table 35: Performance Expectations and Assessment of DHS Progress in Acquisition Management**

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Assess and organize acquisition functions to meet agency needs | *GAO findings:* DHS has taken positive steps to assess and organize acquisition functions within the department to meet agency needs, but more work remains. For example, the department has developed an acquisition oversight plan that it expects to be fully implemented during fiscal year 2007. The Chief Procurement Officer has taken several actions to implement the plan—which generally incorporates basic principles of an effective and accountable acquisition function. The plan monitors acquisition performance through four recurring reviews: self-assessment, operational status, on-site, and acquisition planning. Each component has completed the first self-assessment, which has helped components to identify and prioritize acquisition weaknesses. In addition, each component has submitted an initial operational status report to the Chief Procurement Officer and on-site reviews are being conducted. However, the plan is in the process of being implemented, and is just one of the mechanisms to oversee DHS acquisitions. For example, there is a separate investment review process established to oversee major, complex acquisitions. Regarding the organization of the acquisition function, the October 2004 management directive entitled "Acquisition Line of Business Integration and Management" provided the department's principal guidance for "leading, governing, integrating, and managing" the acquisition function. This directive states that DHS will create departmentwide acquisition policies and procedures and continue to consolidate and integrate the number of systems supporting the acquisition function. However, our prior work found that the Chief Procurement Officer's enforcement authority over procurement decisions at the component agencies was unclear. In addition, according to the directive, the Coast Guard and Secret Service were exempt from complying with the management directive. DHS officials have stated that they are in the process of modifying the lines of business management directive to ensure that no contracting organization is exempt. DHS stated that the Under Secretary for Management has authority as the Chief Acquisition Officer to monitor acquisition performance, establish clear lines of authority for making acquisition decisions, and manage the direction of acquisition policy for the department. They further stated that these authorities devolve to the Chief Procurement Officer. In addition, DHS reported significant progress in staffing of the Office of the Chief Procurement Officer and stated that these additional personnel will significantly contribute to improvement in the DHS acquisition and contracting enterprise. For more information, see *Progress and Challenges in Implementing the Department's Acquisition Oversight Plan,* GAO-07-900; *Ongoing Challenges in Creating an Effective Acquisition Organization,* GAO-07-948T; *Interagency Contracting: Improved Guidance, Planning, and Oversight Would Enable the Department of Homeland Security to Address Risks,* GAO-06-996; *Homeland Security: Further Action Needed to Promote Successful Use of Special DHS Acquisition Authority,* GAO-05-136; *Homeland Security: Challenges in Creating an Effective Acquisition Organization,* GAO-06-1012T; and *Homeland Security: Successes and Challenges in DHS's Efforts to Create an Effective Acquisition Organization,* GAO-05-179.<br>*DHS updated information:* DHS provided additional information on its efforts to assess and organize acquisition functions. For example, DHS reported the Chief Procurement Officer has some means to influence components compliance with procurement policies and procedures. DHS also reported that the Chief Procurement Officer meets monthly with the Component Heads of Contracting Activities to discuss and address issues and common problems. According to DHS, the Chief Procurement Officer has asked the | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | component heads to align their performance goals with the Chief Procurement Officer goals and has direct input into components' performance assessments. DHS reported that the Chief Procurement Officer is developing a series of common metrics to assess the status of acquisition activities within DHS. In addition, the Under Secretary for Management testified that he is examining the authorities of the Chief Procurement Officer to determine whether any change is needed.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. Modifying the acquisition lines of business management directive to ensure that no DHS contracting organization is exempt is a positive step. However, until DHS formally designates the Chief Acquisition Officer, and modifies applicable management directives to support this designation, DHS's existing policy of dual accountability between the component heads and the Chief Procurement Officer leaves unclear the Chief Procurement Officer's authority to enforce corrective actions to achieve the department's acquisition goals. | |
| 2. Develop clear and transparent policies and processes for all acquisitions | *GAO findings:* DHS has not yet developed clear and transparent policies and processes for all acquisitions. For example, DHS put into place an investment review process that adopts many acquisition best practices to help the department reduce risk and increase the chances for successful investment in terms of cost, schedule, and performance. However, in 2005, we found that the process did not include critical management reviews to help ensure that the design for the product performs as expected and that resources match customer needs before any funds are invested. Our prior work on large DHS acquisition programs, such as TSA's Secure Flight program and the Coast Guard's Deepwater program, highlight the need for improved oversight of contractors and adherence to a rigorous management review process. The investment review process is still under revision and the department's performance and accountability report for fiscal year 2006 stated that DHS will incorporate changes to the process by the first quarter of fiscal year 2008. In addition, we found that DHS does not have clear guidance for all types of acquisitions, such as how to manage the risks of interagency contracting. The management of this contracting method was identified as a governmentwide high-risk area in 2005 as a result of improper use. For more information, see GAO-07-948T; GAO-06-996; GAO-06-1012T; and GAO-05-179.<br>*DHS updated information:* DHS provided us with updated information on its efforts to develop clear policies and processes for acquisitions. DHS reported that the department has been working to integrate its organizations through common policies and procedures under the Homeland Security Acquisition Regulation and the *Homeland Security Acquisition Manual*. DHS also reported that the Chief Procurement Officer works with the Component Heads of Contracting Activities to ensure all acquisitions are handled according to DHS policies and procedures.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS did not provide us with documentation of its efforts to ensure that all acquisitions follow DHS's policies and procedures and address challenges we previously identified in DHS's acquisition process. For example, DHS did not report progress on efforts to address weaknesses we identified in its investment review process, including the lack of critical management reviews to help ensure that the design of the product performs as expected and that resource match customer needs. We also reported that DHS lacked guidance for managing certain types of acquisitions, such as how to manage interagency contracting risks, and DHS did not provide us with updated guidance. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 3. Develop an acquisition workforce to implement and monitor acquisitions | *GAO findings:* DHS has taken initial steps needed to develop a workforce to ensure that acquisitions are effectively implemented and monitored, but more work remains. Our reviews have found staffing shortages led the Office of Procurement Operations to rely extensively on outside agencies for contracting support in order to meet contracting needs of several component organizations. Our work on contracting issues following Hurricane Katrina indicated that the number of contract monitoring staff available was not always sufficient, nor were they effectively deployed to provide sufficient oversight. Based on work at the U.S. Immigration and Naturalization Service, in July 2003, we recommended that DHS develop a data-driven assessment of the department's acquisition personnel, resulting in a workforce plan that would identify the number, location, skills, and competencies of the workforce. In 2005, we reported on disparities in the staffing levels and workload imbalance among the component procurement offices. We recommended that DHS conduct a departmentwide assessment of the number of contracting staff, and if a workload imbalance were to be found, take steps to correct it by realigning resources. In 2006, DHS reported significant progress in providing staff for the component contracting offices, though much work remained to fill the positions with qualified, trained acquisition professionals. DHS has established a goal of aligning procurement staffing levels with contract spending at its various components by the last quarter of fiscal year 2009. For more information, see *Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System,* GAO-06-618; *Contract Management: INS Contracting Weaknesses Need Attention from the Department of Homeland Security,* GAO-3-799; GAO-06-996; and GAO-05-179.<br>*DHS updated information:* DHS provided us with additional information on its efforts to develop an acquisition workforce. DHS reported that it authorized the Office of the Chief Procurement Officer 25 full-time equivalents for fiscal year 2007 and has requested an additional 25 full-time equivalents for fiscal year 2008. According to DHS, these additional full-time equivalents will allow the Chief Procurement Officer to complete staffing of its procurement oversight and management functions and provide staff for other acquisition functions, such as program management and cost analysis. In addition, DHS reported that it requested funding in fiscal year 2008 to establish a centrally managed acquisition intern program and provide acquisition training to the DHS acquisition workforce.<br>*Our assessment:* We conclude that DHS generally has not achieved this performance expectation. DHS has much work to fill approved positions and has not corrected workload imbalances among component organizations. | Generally not achieved |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

## DHS Has Made Modest Progress in Financial Management

Effective financial management is a key element of financial accountability. With its establishment by the Homeland Security Act of 2002, DHS inherited a myriad of redundant financial management systems from 22 diverse agencies, along with about 100 resource management systems and 30 reportable conditions identified in prior component financial audits. Additionally, most of the 22 components that transferred to DHS had not been subjected to significant financial statement audit scrutiny prior to their transfer, so the extent to which additional significant internal control deficiencies existed was unknown. DHS's Office of the Chief Financial Officer is responsible for functions, such as budget, finance and accounting, strategic planning and evaluation, and financial systems for the department. The Office of the Chief Financial Officer is also charged with ongoing integration of these functions within the department. For fiscal year 2006, DHS was again unable to obtain an opinion on its financial statements, and numerous material internal control weaknesses continued to be reported. DHS's auditor had issued a disclaimer of opinion on DHS's fiscal years 2003, 2004, and 2005 financial statements.

As shown in table 36, we identified seven performance expectations for DHS in the area of financial management and found that overall DHS has made modest progress meeting those performance expectations. Specifically, we found that DHS has generally achieved two performance expectations and has generally not achieved five others.

Table 36: Performance Expectations and Progress Made in Financial Management

| | Assessment | | |
|---|---|---|---|
| Performance expectation | Generally achieved | Generally not achieved | No assessment made |
| 1. Designate a department Chief Financial Officer who is appointed by the President and confirmed by the Senate | ✓ | | |
| 2. Subject all financial statements to an annual financial statement audit | | ✓ | |
| 3. Obtain an unqualified financial statement audit opinion | | ✓ | |
| 4. Substantially comply with federal financial management system requirements, applicable federal accounting standards, and the U.S. Standard General Ledger at the transaction level | | ✓ | |
| 5. Obtain an unqualified opinion on internal control over financial reporting | | ✓ | |
| 6. Prepare corrective action plans for internal control weaknesses | ✓ | | |
| 7. Correct internal control weaknesses | | ✓ | |
| **Total** | **2** | **5** | **0** |

Source: GAO analysis.

Note: An assessment of “generally achieved” indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of “generally achieved” does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, “generally not achieved” indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of “generally not achieved” may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated “no assessment made.”

Table 37 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of financial management and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation’s key elements (generally not achieved).

Table 37: Performance Expectations and Assessment of DHS Progress in Financial Management

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Designate a department Chief Financial Officer who is appointed by the President and confirmed by the Senate | *GAO and DHS IG findings and our assessment:* DHS has designated a Chief Financial Officer appointed by the President on January 18, 2006, and confirmed by the Senate on May 26, 2006. In July 2004, we noted that with the size and complexity of DHS and the many significant financial management challenges it faces, it is important that DHS's Chief Financial Officer be qualified for the position, displays leadership characteristics, and is regarded as part of DHS's top management. This is because the Chief Financial Officer Act requires, among other things, that the agency's Chief Financial Officer develop and maintain an integrated accounting and financial management system that provides for complete, reliable, and timely financial information that facilitates the systematic measurement of performance at the agency, the development and reporting of cost information, and the integration of accounting and budget information. The Chief Financial Officer is also responsible for all financial management personnel and all financial management systems and operations, which in the case of DHS would include the component Chief Financial Officers and their staff. For more information, see *Department of Homeland Security: Financial Management Challenges,* GAO-04-945T. | Generally achieved |
| 2. Subject all financial statements to an annual financial statement audit | *GAO and DHS IG findings:* DHS has not subjected all financial statements to an annual financial statement audit. According to DHS's fiscal year 2006 Performance and Accountability Report, the DHS IG engaged an independent auditor to audit the September 30, 2006, balance sheet and statement of custodial activity only. According to the Independent Auditor's Report, DHS is to represent that its balance sheet is fairly stated and obtain at least a qualified opinion before it is practical to extend the audit to other financial statements. The Office of Financial Management, Coast Guard, TSA, FEMA, ICE, and the DHS Management Directorate were unable to provide sufficient evidence to support account balances presented in the financial statements and collectively contributed to the auditors' inability to render an opinion for fiscal year 2006. According to the DHS's financial audit results, many of the department's difficulties in financial management and reporting could be attributed to the original stand-up of a large, new, and complex executive branch agency without adequate organizational expertise in financial management and accounting. DHS recently committed to obtaining additional human resources and other critical infrastructure necessary to develop reliable financial processes, policies, procedures, and internal controls to enable management to represent that financial statements are complete and accurate. For more information, see Department of Homeland Security Office of Inspector General, *Independent Auditors' Report on DHS' FY 2006 Financial Statements,* OIG-07-10 (Washington, D.C.: November 2006).<br>*DHS updated Information:* DHS did not provide updated information relating to this performance expectation. In March 2007, DHS officials indicated that they generally agreed with our assessment and noted that the department has determined that it is not an effective use of resources to subject all financial statements to an annual audit until its balance sheet receives an unqualified opinion.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. According to the DHS fiscal year 2006 Performance and Accountability Report and audits conducted by the DHS IG and independent auditors that DHS has not subjected all of its financial statements to an annual financial statement audit. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 3. Obtain an unqualified financial statement audit opinion | *GAO and DHS IG findings:* For fiscal year 2006, DHS was unable to obtain an opinion on its financial statements, and numerous material internal control weaknesses continued to be reported. Independent auditors under contract with the DHS IG issued a disclaimer of opinion on DHS's fiscal year 2004, 2005, and 2006 financial statements. The disclaimer of opinion was due primarily to financial reporting problems at four component agencies and at the department level. In September 2003, we noted that although many of the larger agencies that transferred to DHS had been able to obtain unqualified, or "clean," audit opinions on their annual financial statements, most employed significant effort and manual workarounds to do so in order to overcome a history of poor financial management systems and significant internal control weaknesses. For more information, see Department of Homeland Security Office of Inspector General, *Fiscal Year 2006 DHS Performance and Accountability Report* (Washington, D.C.: 2006) and *Department of Homeland Security: Challenges and Steps in Establishing Sound Financial Management,* GAO-03-1134T.<br>*DHS updated information:* In March 2007, DHS provided updated information about progress component agencies had made in audits of their financial statements. DHS stated that CBP underwent a full scope, standalone audit of its fiscal year 2006 financial statements and received an unqualified audit opinion, and that the Federal Law Enforcement Training Center achieved an unqualified opinion of its first balance sheet audit. However, DHS officials stated that the department will likely not be able to obtain an unqualified opinion on its financial statements, primarily because of material weaknesses at the Coast Guard. According to the DHS Office of the Chief Financial Officer, the Coast Guard has a material weakness in virtually every category and has not yet addressed many of the root causes of these weaknesses, including insufficient policies and procedures and lack of effective control systems. With regard to other DHS components, the Office of the Chief Financial Officer noted that in the fiscal year 2006 audit report, the auditors dropped several material conditions that were reported in the fiscal year 2005 report, indicating that DHS has made progress in addressing some material weaknesses. For example, during fiscal year 2006, the Office of the Chief Financial Officer noted that ICE and TSA made significant progress in addressing their material weaknesses and are projected to make more progress in fiscal year 2007. According to DHS officials, the Coast Guard also established a Financial Management Transformation Task Force in July 2006 through which the Coast Guard developed milestones to address its financial management challenges. In addition, the Office of the Chief Financial Officer noted that the department has faced challenges in ensuring the development and implementation of effective control systems due to the multiple departmental reorganizations since its establishment 4 years ago. For more information, see Department of Homeland Security Office of Inspector General, *Independent Auditors' Report on CBP's FY 2006 Consolidated Financial Statements,* OIG-07-19 (Washington, D.C.: December 2006) and Department of Homeland Security Office of Inspector General, *Special Report: Letter on Information Technology Matters Related to TSA's FY 2005 Financial Statements (Redacted),* OIG-07-18 (Washington, D.C.: December 2006).<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Some DHS components have recently made progress in their component financial statement and balance sheet audits, but substantial more work remains, as DHS has not yet obtained an unqualified opinion on its financial statement. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 4. Substantially comply with federal financial management system requirements, federal accounting standards, and the U.S. Standard General Ledger at the transaction level | *GAO and DHS IG findings:* DHS has not yet ensured that it substantially complies with the Federal Financial Management Systems Requirements, Federal Accounting Standards, and the U.S. Standard General Ledger at the transaction level. In 2006, we reported that the eMerge2 program was supposed to provide DHS with the financial system functionality to consolidate and integrate the department's financial accounting and reporting systems, including budget, accounting and reporting, cost management, asset management, and acquisition and grants functions, thereby helping the department comply with the Federal Financial Management Systems Requirements, Federal Accounting Standards, and the U.S. Standard General Ledger at the transaction level. We noted that DHS officials stated that a systems integrator was hired in December 2003, and the project was expected to be fully deployed and operational in 2006. According to DHS officials, because the project was not meeting its performance goals and timeline, DHS officials began considering whether to continue the project and in spring 2005 started looking at another strategy. Further, we reported that DHS officials decided to change the strategy for the eMerge2 program in October 2005 and focus on leveraging the systems already in place. DHS planed to continue eMerge2 using a shared services approach. According to DHS officials, although a departmentwide concept of operations and migration plan were still under development, they expected progress to be made in the next 5 years. We reported that DHS officials said that they had decided to develop a new strategy for the planned financial management systems integration program because the prior strategy was not meeting its performance goals and timeline. For more information, see *Financial Management Systems: DHS Has an Opportunity to Incorporate Best Practices in Modernization Efforts,* GAO-06-553T. Also, see Department of Homeland Security Office of Inspector General, *Fiscal Year 2006 DHS Performance and Accountability Report* (Washington, D.C.: 2006).<br>*DHS updated information:* In March 2007, DHS provided us with updated information on components' efforts to comply with Federal Financial Management System Requirements, Federal Accounting Standards, and the U.S. Standard General Ledger at the transaction level. In October 2004, CBP successfully implemented, on schedule, its third and last phase of its financial system. According to DHS, the system replaced several legacy systems and provides CBP with a fully integrated system for budget, acquisition, finance, and property and therefore helping to ensure CBP's compliance with the Federal Financial Management Systems Requirements, Federal Accounting Standards, and the U.S. Standard General Ledger at the transaction level. DHS further noted that this successful implementation was an integral part of CBP obtaining an unqualified audit opinion.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS is still in the process of developing a new strategy for integrating its financial management systems, but departmentwide has not yet substantially compiled with Federal Financial Management System Requirements, Federal Accounting Standards, and the U.S. Standard General Ledger at the transaction level. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 5. Obtain an unqualified opinion on internal control over financial reporting | *GAO and DHS IG findings:* DHS is required by the DHS Financial Accountability Act to obtain an opinion on its internal control over financial reporting. According to DHS's fiscal year 2006 Performance and Accountability Report, the DHS IG issued an adverse opinion. During fiscal year 2006, the auditors identified the following reportable conditions, which are considered material weaknesses: financial management oversight (entity level controls); financial reporting; financial systems security; fund balance with Treasury; property, plant, and equipment; operating materials and supplies; legal and other liabilities; actuarial liabilities; budgetary accounting; and intragovernmental and intradepartmental balances. For more information, see Department of Homeland Security Office of Inspector General, *FY 2006 Audit of DHS' Internal Control Over Financial Reporting,* OIG-07-20 (Washington, D.C.: December 2006) and Department of Homeland Security Office of Inspector General, *Review of FEMA Internal Controls for Funding Administrative Cost Under State Management Grants,* OIG-07-21(Washington, D.C.: December 2007).<br>*DHS updated information:* DHS did not provide us with updated information on its efforts to obtain an unqualified opinion on internal control over financial reporting.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation, as DHS has not yet obtained an unqualified opinion on internal control over financial reporting. | Generally not achieved |
| 6. Prepare corrective action plans for internal control weaknesses | *GAO and DHS IG findings:* DHS has taken steps to prepare corrective action plans for internal control weaknesses. According to the fiscal year 2006 DHS Performance and Accountability Report, during 2006, DHS reported formalizing the corrective action planning process through a management directive, guidance, and training; implementing an automated corrective action tracking system to ensure progress is tracked and management is held accountable for progress; developing a corrective action strategic planning process for improving financial management at DHS; working with the Office of Management and Budget to monitor corrective action plans; establishing ongoing reporting by the DHS IG that assesses and complements management's corrective action efforts through performance audits; and executing the first phase of the Office of Management and Budget-approved multiyear plan to implement a comprehensive internal control assessment pursuant to the Office of Management and Budget Circular No. A-123, Appendix A, Management's Responsibility for Internal Control, guidelines. However, according to the fiscal year 2006 DHS Performance and Accountability Report, DHS and its components did not fully develop corrective action plans to address all material weaknesses and reportable conditions identified by previous financial statement audits. In the past, the DHS IG noted that some corrective action plans lacked sufficient detail, such as clearly defined roles and responsibilities, actions to be taken, timetables for completion of actions, and documented supervisory review and approval of completed actions. For more information, see Department of Homeland Security Office of Inspector General, *Audit of DHS' Corrective Action Plan Process for Financial Reporting, Report No. 4,* OIG-07-29 (Washington, D.C.: February 2007) and *Audit of DHS' Corrective Action Plan Process for Financial Reporting - Report No. 3,* OIG-07-13 (Washington, D.C.: December 2006).<br>*DHS updated information:* In April 2007, DHS provided us with updated information on its efforts to develop corrective action plans. According to DHS, a departmentwide committee has been working since January 2006 to develop its first departmentwide Corrective Action Plan, which it refers to as its Internal Controls over Financial Reporting Playbook Fiscal Year 2007. The department started its corrective action planning process in November 2005 by holding internal meetings and initiating the procurement process to obtain a contractor to develop a tracking system for the department's corrective action plans. Additionally, beginning in December 2005, DHS held meetings with its components, including the Coast Guard and ICE, to develop corrective action plans and establish financial management remediation issues for fiscal year 2006. Throughout 2006, the DHS Chief Financial Officer | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | held approximately 12 corrective action plan workshops with the component agencies regarding areas of focus for improving financial management and stressing the importance of identifying and addressing the root causes of component agencies' financial management weaknesses. Additionally, the department has developed reports to illustrate progress in corrective action planning on a quarterly basis.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS has taken actions to develop corrective action plans by, for example, developing and issuing a departmentwide plan for the corrective action plan process and holding workshops or corrective action plans. | |
| 7. Correct internal control weaknesses | *GAO and DHS IG findings:* DHS and its components have not fully implemented corrective action plans to address all material weaknesses and reportable conditions identified by previous financial statement audits. In its fiscal year 2006 Performance and Accountability Report, DHS reported on planned corrective actions to address materials weaknesses in internal controls over financial reporting and established target dates for completing the corrections. In addition, the DHS IG reported that progress in implementing corrective action plans among DHS component agencies was mixed. For more information, see Department of Homeland Security Office of Inspector General, *Audit of DHS' Corrective Action Plan Process for Financial Reporting, Report No. 4,* OIG-07-29 (Washington, D.C.: February 2007) and *Audit of DHS' Corrective Action Plan Process for Financial Reporting - Report No. 3,* OIG-07-13 (Washington, D.C.: December 2006).<br>*DHS updated information:* DHS did not provide updated information relating to this performance expectation but DHS officials indicated that they generally agreed with our assessment, and that DHS has not yet corrected its internal control weaknesses. The Office of the Chief Financial Officer noted that while DHS addressed many weaknesses during fiscal year 2006 and, as shown in the Internal Controls over Financial Reporting Playbook, plans to address these weaknesses through fiscal year 2010, it will likely take DHS until fiscal year 2010 to address all of its weaknesses because of pervasive financial management problems at the Coast Guard. According to DHS officials, the Coast Guard has made some progress, establishing a Financial Management Transformation Task Force in July 2006 through which the Coast Guard developed milestones to address its financial management challenges. Office of the Chief Financial Officer officials stated that DHS has developed goals and milestones for addressing its material weaknesses and reportable conditions in the Electronic Program Management Office, a project management tool that is supposed to help improve communication on activities in component offices, ensure accountability, and enhance the department's ability to react quickly to meet mission-critical objectives.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has not yet corrected internal control weaknesses, according to the department, the DHS IG, and independent auditors. | Generally not achieved |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

## DHS Has Made Limited Progress in Managing Human Capital

Key human capital management areas for all agencies, including DHS, are pay, performance management, classification, labor relations, adverse actions, employee appeals, and diversity management. Congress provided DHS with significant flexibility to design a modern human capital management system. DHS and the Office of Personnel Management jointly released the final regulations on DHS's new human capital system in February 2005. The final regulations established a new human capital system for DHS that was intended to ensure its ability to attract, retain, and reward a workforce that is able to meet its critical mission. Further, the human capital system provided for greater flexibility and accountability in the way employees are to be paid, developed, evaluated, afforded due process, and represented by labor organizations while reflecting the principles of merit and fairness embodied in the statutory merit systems principles. Although DHS intended to implement the new personnel system in the summer of 2005, court decisions enjoined the department from implementing certain labor management portions of it. Since that time, DHS has taken actions to implement its human capital system and issued its Fiscal Year 2007 and 2008 Human Capital Operational Plan in April 2007.

As shown in table 38, we identified eight performance expectations for DHS in the area of human capital management and found that overall DHS has made limited progress in meeting those performance expectations. Specifically, we found that DHS has generally achieved two performance expectations and has generally not achieved six other expectations.

Table 38: Performance Expectations and Progress Made in Human Capital Management

| | Assessment | | |
|---|---|---|---|
| Performance expectation | Generally achieved | Generally not achieved | No assessment made |
| 1. Develop a results-oriented strategic human capital plan | ✓ | | |
| 2. Implement a human capital system that links human capital planning to overall agency strategic planning | | ✓ | |
| 3. Develop and implement processes to recruit and hire employees who possess needed skills | | ✓ | |
| 4. Measure agency performance and make strategic human capital decisions | | ✓ | |
| 5. Establish a market-based and more performance-oriented pay system. | | ✓ | |
| 6. Seek feedback from employees to allow for their participation in the decision-making process | | ✓ | |
| 7. Create a comprehensive plan for training and professional development | ✓ | | |
| 8. Implement training and development programs in support of DHS's mission and goals | | ✓ | |
| **Total** | 2 | 6 | 0 |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

Table 39 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of human capital management and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation's key elements (generally not achieved).

Table 39: Performance Expectations and Assessment of DHS Progress in Human Capital Management

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Develop a results-oriented strategic human capital plan | *GAO findings:* DHS has developed a results-oriented strategic human capital plan and issued its human capital strategic plan in October 2004. In September 2005 we reported that the plan includes selected training strategies, such as developing a leadership curriculum to ensure consistency of organizational values across the department and using training to support the implementation of the DHS human capital management system. We also reported that it provides an illustration of one way to communicate linkages between goals and strategies contained in the plan and the broader organizational goals they are intended to support. For more information see *Department of Homeland Security: Strategic Management of Training Important for Successful Transformation,* GAO-05-888 and *Human Capital: DHS Faces Challenges In Implementing Its New Personnel System,* GAO-04-790.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information related to this performance expectation. In addition to its strategic human capital plan, DHS has developed a fiscal year 2007 and 2008 Human Capital Operational Plan, which provides specific measurable goals that the department is using to gauge the effectiveness of the its human capital efforts<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation, as it has developed a strategic human capital plan. | Generally achieved |
| 2. Implement a human capital system that links human capital planning to overall agency strategic planning | *GAO findings:* DHS has taken steps to implement a human capital system that links human capital planning to overall agency strategic planning, but more work remains. For example, federal court decisions have enjoined the department from implementing the labor management portions of its human capital system. We reported in September 2005 that human capital management system, known at that time as MAX$^{HR}$, represented a fundamental change in many of the department's human capital policies and procedures that would affect a large majority—approximately 110,000—of its civilian employees. MAX$^{HR}$ covered many key human capital areas, such as pay, performance management, classification, labor relations, adverse actions, and employee appeals. For more information see GAO-05-888; *Human Capital: Observations on Final DHS Human Capital Regulations,* GAO-05-391T; GAO-04-790; and *Human Capital: DHS Personnel System Design Effort Provides for Collaboration and Employee Participation,* GAO-03-1099.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to implement a human capital system that links human capital planning to overall agency strategic planning. DHS has developed the Human Capital Operational Plan, which identifies five department priorities—hiring and retaining a talented and diverse workforce; creating a DHS-wide culture of performance; creating high-quality learning and development programs for DHS employees; implementing a DHS-wide integrated leadership system; and being a model of human capital service excellence. DHS told us that the Human Capital Operational Plan encompasses the initiatives of the previous human capital management system, MAX$^{HR}$, but represents a more comprehensive human resources program. The Human Capital Operational Plan identifies 77 goals for the department to achieve throughout fiscal years 2007 and 2008, and DHS has met the 8 goals with target dates of April 30, 2007, or earlier. For example, DHS has developed a hiring model, developed a communication plan for the Human Capital Operational Plan, and equipped components with a service level agreement model. DHS also reported that its Performance Management Program has been expanded and continues to be expanded across the department and is an integral part in DHS's strategy for building a single, unified department and linking individual performance with specific organizational goals. DHS stated that since deployment of the | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | Performance Management Program to bargaining unit employees will require collective bargaining, further expansion is proceeding as appropriate and that once negotiation is complete at the component level, the new program will be rolled out to both bargaining unit and non-bargaining unit employees at the same time.<br>*Our assessment:* We conclude that DHS has generally not achieved this expectation. While DHS has taken actions to implement a human capital system that links human capital planning to overall agency strategic planning, more work remains. DHS has issued the Human Capital Operational Plan, which identifies department priorities and goals for fiscal years 2007 and 2008. While DHS has met goals with target dates of April 30, 2007, or earlier, the vast majority of goals set out in the Human Capital Operational Plan have target dates after April 30, 2007. DHS reported that it is on track to meet future goals, but the goals have not yet been met. | |
| 3. Develop and implement processes to recruit and hire employees who possess needed skills | *GAO findings:* DHS has faced difficulties in developing and implementing processes to recruit and hire employees who possess needed skills. We have noted that hiring or staffing difficulties have adversely affected DHS operations in various areas, including border security and immigration enforcement, aviation security, emergency preparedness and response, and acquisition management. For example, in May 2005 we reported that ineffective DHS management processes have impeded the department's ability to hire employees and maintain contracts. In September 2006 we reported that concerns regarding staffing for disaster response management have been longstanding, and we noted that FEMA officials cited the lack of agency and contractor staffing as a difficulty. We also reported that DHS's Office of the Chief Procurement Officer has not focused on oversight due in part to limited staffing. In addition, in January 2007 we reported that FEMA lacks a strategic workforce plan and related human capital strategies—such as succession planning or a coordinated training effort. Such tools are integral to managing resources, as they enable an agency to define staffing levels, identify the critical skills needed to achieve its mission, and eliminate or mitigate gaps between current and future skills and competencies. For more information see *Budget Issues: FEMA Needs Adequate Data, Plans, and Systems to Effectively Manage Resources for Day-to-Day Operations,* GAO-07-139; *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity,* GAO-06-1087T; *Homeland Security: Visitor and Immigrant Status Program Operating, but Management Improvements Are Still Needed,* GAO-06-318T; *Immigration Benefits: Improvements Needed to Address Backlogs and Ensure Quality of Adjudications,* GAO-06-20; *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities,* GAO-05-434; *Information Technology: Homeland Security Should Better Balance Need for System Integration Strategy with Spending for New and Enhanced Systems,* GAO-04-509; and *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed,* GAO-03-1083.<br>*DHS updated information:* In March, April, and May 2007, DHS provided us with updated information on its efforts to develop and implement processes to recruit and hire employees who possess needed skills. In the Human Capital Operational Plan, DHS identifies a number of goals and target dates concerning hiring and recruitment, such as implementing DHS-wide recruitment strategies and establishing an intern program for specific occupations. DHS has met two of the plan's hiring goals and associated target dates—developing/benchmarking a hiring model and developing training on the hiring model. DHS's 45-day hiring model has 20 steps, such as posting a vacancy announcement and checking references, and 8 of the steps are measured for the purposes of the 45-day target.<br>DHS stated that the hiring model has been provided to all components and that it | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | receives regular reporting from components against the 45-day hiring target. DHS reported that it is on track to meet the July target date for assessing hiring practices against the hiring model and stated that it is on schedule to meet target dates for other future goals as well. For example, DHS stated that it is in the process of developing e-Recruitment, an enterprise-wide tool for application processing and workforce planning.<br>*Our assessment:* We conclude that this performance expectation has generally not been achieved. While DHS has taken steps to develop processes to recruit and hire employees who possess needed skills, more work remains. For example, DHS has developed a hiring model, but the department has not yet assessed the component's practices against it. DHS is also still in the process of meeting other recruitment and hiring goals, such as the deployment of e-Recruitment and the establishment of an intern program in specific occupations. | |
| 4. Measure agency performance and make strategic human capital decisions | *GAO findings:* DHS has not yet taken the steps needed to measure performance and make strategic human capital decisions. In June 2004, we reported that DHS headquarters has not yet been systematic or consistent in gathering relevant data on the successes or shortcomings of legacy component human capital approaches or current and future workforce challenges, despite the potential usefulness of this information to strategic human capital planning activities. We reported that efforts were under way to gather such data. For more information see GAO-05-391T and GAO-04-790.<br>*DHS updated information:* In March, April, and May 2007, DHS provided us with updated information on its efforts to measure agency performance and make strategic human capital decisions. Specifically, DHS stated that its human capital accountability plan has been distributed, approved by the Office of Personnel Management, and is operational but not final. This plan will outline the department's strategy for monitoring and evaluating its human capital policies and programs and for conducting cyclical compliance audits of human resources management operations. DHS also reported that it has identified component representatives to serve on audit teams for accountability that will specialize in human resources issues. DHS plans to audit the Coast Guard this year. Further, DHS stated that it is currently working with components to develop metrics for human capital management. DHS stated that these metrics will revolve around hiring, talent, leadership, and accountability. DHS reported that the department has put together an initial framework for these metrics and hopes to have some in use by October 2007. DHS also stated that since 2005, the DHS Human Capital Office has served on the DHS Chief Financial Officer's Internal Controls Committee. DHS reported that GAO's Internal Control Management Tool has been used each year to collect and review DHS-wide responses and develop corrective action plans, including data on the many Human Capital-related questions within this tool. DHS stated that DHS Chief Financial Officer tracks and reports the compiled data to the Office of Management and Budget.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has made efforts to measure agency performance and make strategic human capital decisions. However, these efforts are not yet complete. For example, DHS's human capital accountability plan is operational but not yet final, and the department has not finalized metrics it will use for human capital management. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 5. Establish a market-based and more performance-oriented pay system | *GAO findings:* DHS has not yet established a market-based and more performance-oriented pay system. In 2005 we testified that the final regulations on DHS's human capital system provided for a flexible, contemporary, performance-oriented, and market-based compensation system. Specifically, DHS planned to establish occupational clusters and pay bands and may, after coordination with the Office of Personnel Management, set and adjust pay ranges—taking into account mission requirements, labor market conditions, availability of funds, and other relevant factors. While the final regulations contained many elements of a market-based and performance-oriented pay system, there were several issues that we identified that DHS needed to continue to address as it moved forward with the implementation of the system. These issues included linking organizational goals to individual performance, using competencies to provide a fuller assessment of performance, making meaningful distinctions in employee performance, and continuing to incorporate adequate safeguards to ensure fairness and guard against abuse. For more information, see GAO-05-391T<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to establish a market-based and more performance-oriented pay system. DHS reported that it is developing implementation plans to conduct a performance-based pay pilot program in a component or organization in order to validate, measure, and refine the pay band models and processes developed. DHS stated that the steps required for implementation of a pilot program have been identified and reported that as an initial step in that process it is identifying a group that would serve as a reasonable sample for an assessment of DHS's pay band model and pay administration procedures. Further, DHS stated that it is assessing the budget implications for implementation and taking the steps necessary to ensure availability of sufficient funding. DHS also told us that it has developed competencies for 115 occupations. DHS stated that the competencies will be validated by August 2007 and implemented in September 2007.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. While DHS has taken steps to develop a market-based and more performance-oriented pay system, the department has not yet established such a system. The department reported that it is developing a pilot program but that this program is still in the planning stages. | Generally not achieved |
| 6. Seek feedback from employees to allow for their participation in the decision-making process. | *GAO findings:* While DHS has taken steps to seek feedback from employees to allow them to be involved in the decision-making process, more work remains. In September 2003, for example, we reported that employee perspectives on the design of the DHS human capital system, formerly known as MAX$^{HR}$, were sought through many mechanisms. Activity updates were provided in the DHS weekly newsletter, an e-mail mailbox for employees to submit their suggestions and comments was used, and multiple town hall meetings and focus groups conducted between the end of May and the beginning of July 2003 were held in 10 cities across the United States. However, in June 2004 we pointed to challenges in implementing the human capital system in a collaborative way. We reported that regardless of whether it is a part of collective bargaining, involving employees in such important decisions as how they are deployed and how work is assigned is critical to the successful operation of the department. This is likely to be a significant challenge in light of employee responses to the 2006 U.S. Office of Personnel Management Federal Human Capital Survey in which about 30 percent of DHS employees indicated a feeling of personal empowerment, which is less than the governmentwide response of about 42 percent. Additionally, about 39 percent of DHS employees reported satisfaction with their involvement in decisions that affect their work, compared to about 54 percent governmentwide. For more information, see GAO-05-391T; GAO-04-790; and GAO-03-1099. | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | *DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to seek feedback from employees to allow for their participation in the decision-making process. DHS reported that it is expanding its communication strategy, including an enhanced DHS human capital Web site. Further, DHS reported that in consultation with the Undersecretary for Management, component heads, and the DHS Human Capital Council, it developed an overall strategy for addressing employee concerns as reflected in the Federal Human Capital Survey results, and the department reported that it has already completed a number of actions to address the issues raised in the 2006 Federal Human Capital Survey, as well as the findings of the Common Culture Task Force. For example, DHS stated that it is continuing ongoing focus groups and surveys.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has taken a variety of steps to seek feedback from employees to allow for their participation in the decision-making process, but it continues to face challenges. For example, during the design of $\text{MAX}^{\text{HR}}$, DHS took actions to obtain employees' perspectives through focus groups and town hall meetings. However, the results of the U.S. Office of Personnel Management Federal Human Capital Survey indicate that DHS employees do not perceive that they have had sufficient involvement in decision making at DHS. While DHS reported that it is taking actions to address the concerns raised in the Federal Human Capital Survey, it is too early to evaluate their effectiveness. | |
| 7. Create a comprehensive plan for training and professional development | *GAO findings:* DHS has created a comprehensive plan for training and development. DHS's department-level training strategy is presented in its human capital and training strategic plans. Issued in October 2004, its human capital strategic plan includes selected training strategies, such as developing a leadership curriculum to ensure consistency of organizational values across the department and using training to support the implementation of the DHS human capital management system. In July 2005, DHS issued its first departmental training plan, the Department of Homeland Security Learning and Development Strategic Plan, which provides a strategic vision for departmentwide training. We reported that this plan is a significant and positive step toward addressing departmentwide training challenges. For more information, see GAO-05-888.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to create comprehensive plans for training and professional development. DHS has filled the position of Chief Learning Officer and has developed a draft Learning and Development Strategy. The draft plan provides a strategy for how the department will institutionalize and standardize employee training, education, and professional development, and it also identifies the four pillars of the DHS University System, which include the Leadership Institute, the Preparedness Center, the Homeland Security Academy, and the Center for Academic and Interagency Programs.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation as the department has created a training and professional development plan. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 8. Implement training and development programs in support of DHS's mission and goals | *GAO findings:* While DHS has taken steps to implement training and development programs in support of DHS's mission and goals, it continues to face difficulties. In September 2005, we reported that under the overall direction of the Chief Human Capital Officer office, DHS has established a structure of training councils and groups that cover a wide range of issues and include representatives from each organizational component within DHS. The Training Leaders Council plays a vital role in DHS's efforts to foster communication and interchange among the department's various training communities. DHS has also established a Chief Learning Officer. However, the formation of DHS from 22 legacy agencies and programs has created challenges to achieving departmentwide training goals. Of particular concern to the training officials we spoke with were the lack of common management information systems and the absence of commonly understood training terminology across components. For more information, see GAO-05-888.<br>*DHS updated information:* In March, April, and May 2007, DHS provided us with updated information on its efforts to implement training and development programs in support of DHS's mission and goals. Specifically, DHS has established an Office of Personnel Management-approved Senior Executive Service Candidate Development Program and held the orientation for its initial Senior Executive Service Candidate Development Program class in March 2007. DHS also reported that it has created and launched the National Capital Region Homeland Security Academy. The Academy will offer a fully accredited graduate degree in Homeland Security Studies and, when combined with the West Coast program, will matriculate 200 students annually. Further, DHS reported that it is conducting academic and outreach partnerships with National Defense University, Minority Servicing Institutions, and educational consortiums, such as the National Security Education Consortium and the Homeland Security and Defense Education Consortium. DHS also stated that it is developing electronic courses for employees in need of specific training and plans to roll out these courses in the near future. DHS reported that the DHS Training Leaders Council, a council of training representatives from DHS Components, created a Training Glossary that is used across the department. DHS also reported that on February 5, 2007, the department successfully launched its learning management system, DHScovery. DHS stated that ultimately DHScovery will deliver and track DHS departmentwide employee training events.<br>*Our assessment:* We conclude that DHS generally has not achieved this performance expectation. DHS has made progress in implementing training and development programs in support of DHS's mission and goals. However, most of DHS's training and development goals identified in the *Human Capital Operational Plan* have not yet been fully implemented. | Generally not achieved |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

## DHS Has Made Limited Progress in Information Technology Management

DHS has undertaken efforts to establish and institutionalize the range of information technology management controls and capabilities that our research and past work have shown are fundamental to any organization's ability to use technology effectively to transform itself and accomplish mission goals. Among these information technology management controls and capabilities are

- centralizing leadership for extending these disciplines throughout the organization with an empowered Chief Information Officer,
- having sufficient people with the right knowledge, skills, and abilities to execute each of these areas now and in the future;
- developing and using an enterprise architecture, or corporate blueprint, as an authoritative frame of reference to guide and constrain system investments;
- defining and following a corporate process for informed decision making by senior leadership about competing information technology investment options;
- applying system and software development and acquisition discipline and rigor when defining, designing, developing, testing, deploying, and maintaining systems; and
- establishing a comprehensive, departmentwide information security program to protect information and systems;

Despite its efforts over the last several years, the department has significantly more to do before each of these management controls and capabilities is fully in place and is integral to how each system investment is managed.

As shown in table 40, we identified 13 performance expectations for DHS in the area of information technology management and found that overall DHS has made limited progress in meeting those expectations. In particular, we found that DHS has generally achieved 2 performance expectations and has generally not achieved 8 others. For 3 other performance expectations, we did not make an assessment.

Table 40: Performance Expectations and Progress Made in Information Technology Management

| Performance expectation | Assessment | | |
|---|---|---|---|
| | Generally achieved | Generally not achieved | No assessment made |
| 1. Organize roles and responsibilities for information technology under the Chief Information Officer | ✓ | | |
| 2. Develop a strategy and plan for information technology management | | ✓ | |
| 3. Develop measures to assess performance in the management of information technology | | ✓ | |
| 4. Strategically manage information technology human capital | | | ✓ |
| 5. Develop a comprehensive enterprise architecture | | | ✓ |
| 6. Implement a comprehensive enterprise architecture | | ✓ | |
| 7. Develop a process to effectively manage information technology investments | | ✓ | |
| 8. Implement a process to effectively manage information technology investments | | ✓ | |
| 9. Develop policies and procedures for effective information systems development and acquisition | | ✓ | |
| 10. Implement policies and procedures for effective information systems development and acquisition | | ✓ | |
| 11. Provide operational capabilities for information technology infrastructure and applications | | | ✓ |
| 12. Develop policies and procedures to ensure protection of sensitive information | ✓ | | |
| 13. Implement policies and procedures to effectively safeguard sensitive information | | ✓ | |
| **Total** | **2** | **8** | **3** |

Source: GAO analysis.

Note: An assessment of “generally achieved” indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of “generally achieved” does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, “generally not achieved” indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of “generally not achieved” may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated “no assessment made.”

Table 41 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of information technology management and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation's key elements (generally not achieved).

Table 41: Performance Expectations and Assessment of DHS Progress in Information Technology Management

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Organize roles and responsibilities for information technology under the Chief Information Officer | *GAO findings:* In May 2004, we reported that the DHS Chief Information Officer did not have the authority and control over departmentwide information technology spending. Control over the department's information technology budget was vested primarily with the Chief Information Officer organizations within each DHS component. As a result, DHS's Chief Information Officer did not have authority to manage information technology assets across the department. For more information, see *Homeland Security Progress Continues but Challenges Remain on Department's Management of Information Technology,* GAO-06-598T.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to organize roles and responsibilities under the Chief Information Officer. Specifically, in March 2007 DHS issued a management directive that expanded the authorities and responsibilities of its Chief Information Officer. The directive gives the Chief Information Officer responsibility for and authority over information technology resources, including funding and human capital of DHS's components.<br>*Our assessment:* We conclude that DHS has generally achieved this performance expectation. DHS's March 2007 management directive is consistent with our 2004 recommendation that the department strengthen the Chief Information Officer's authority and control over departmentwide information technology spending. | Generally achieved |
| 2. Develop a strategy and plan for information technology management | *GAO findings:* In 2004 we reported DHS's draft information resource management strategic plan dated March 2004 listed the priorities of the department's and component agencies' Chief Information Officers for 2004. We also reported that the department was in the process of developing what it termed as road maps for each of these priority areas that included descriptions of the current condition of the area, the need for change, the planned future state, initiatives, and barriers. However, we reported that neither DHS's draft information resource management strategic plan nor the draft priority area road maps developed by DHS contained sufficient information regarding the department's information technology goals and performance measures, when the department expected that significant activities would be completed, and the staff resources necessary to implement those activities. For more information, see GAO-06-598T and *Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach,* GAO-04-702.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to develop a strategy for information technology management. In particular, DHS provided us with a document titled the Office of the Chief Information Officer Strategic Plan, Fiscal years 2007-2011. This plan lays out five goals for the department's information technology capabilities and includes information on strategic objectives linked to those goals. The plan's five goals are (1) continuing cyber security improvements; (2) driving information technology operational efficiencies, improvements; and resiliency; (3) aligning information technology planning and budgeting with procurement activities and the enterprise architecture; (4) establishing a foundation for information sharing, data collection, and integration; and (5) establishing and governing a portfolio of cross-departmental information technology capabilities to support DHS mission and management objectives. The plan also aligns the Office of the Chief Information Officer's information technology goals to DHS's mission priorities.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS's Office of the Chief Information Officer Strategic Plan represents a starting | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | point for DHS in its efforts to develop a strategy and plan for information technology management. However, the plan does not include well-developed milestones and clearly defined roles and responsibilities for executing initiatives, which we have previously reported are key elements of a good strategic plan. | |
| 3. Develop measures to assess performance in the management of information technology | *GAO findings:* In 2004 we reported that neither DHS's draft information resource management strategic plan nor the draft priority area road maps developed by DHS contained sufficient information regarding the department's information technology goals and performance measures. We reported that leading organizations define specific goals, objectives, and measures; use a diversity of measurement types; and describe how information technology outputs and outcomes affect organizational customer and agency program delivery requirements. In addition, we reported that the Paperwork Reduction Act and the Clinger-Cohen Act of 1996 requires agencies to establish goals and performance measures on how information and technology management contributes to program productivity, the efficiency and effectiveness of agency operations, and service to the public. More recently, DHS has taken actions consistent with the expectation. Specifically, DHS established key information technology initiatives and associated goals as part of its 2005-2006 Information Technology Strategy. This strategy linked key information technology initiatives and goals to DHS's overarching mission and goals, such as providing service to the public and increasing the efficiency and effectiveness of agency operations and program productivity. For more information, see GAO-04-702.<br>*DHS updated information:* In March and April 2007, DHS provided us with updated information on its efforts to develop performance measures for information technology management. DHS reported that it uses the Office of Management and Budget's Program Assessment Rating Tool to measure the performance if individual information technology programs. DHS also reported that performance measures for major programs are tracked in the Office of Management and Budget Exhibit 300 business cases.<br>*Our assessment:* Until DHS provides evidence that it has developed measures for assessing the department's management of information technology, we conclude that DHS has generally not achieved this performance expectation. DHS reported using various tools to measure performance of individual information technology programs. However, we believe that while the Program Assessment Rating Tool and the Exhibit 300 business cases can help provide important information for the department on the management of individual investments, these tools do not provide measures for routinely assessing overall information technology management performance. | Generally not achieved |
| 4. Strategically manage information technology human capital | *GAO findings and assessment:* We have not conducted work on DHS's information technology human capital management and DHS did not provide us with information on its efforts to achieve this performance expectation that would allow us to make an assessment on DHS's progress in achieving this performance expectation. In the past, we noted that DHS faced difficulties in strategically managing its human capital for information technology. We also reported that DHS had begun strategic planning for information technology human capital at the headquarters level, but it had not yet systematically gathered baseline data about its existing workforce. We have ongoing work in this area and plan to report on the results of this work later this year. For more information, see GAO-06-598T and GAO-04-702. | No assessment made |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 5. Develop a comprehensive enterprise architecture | *GAO findings:* An enterprise architecture provides systematic structural descriptions—in useful models, diagrams, tables, and narrative—of how a given entity operates today and how it plans to operate in the future, and it includes a road map for transitioning from today to tomorrow. The Clinger-Cohen Act and the Office of Management and Budget require that departments such as DHS develop and use an architecture. DHS has begun developing an enterprise architecture using an evolutionary approach that entails producing successively more mature versions. DHS released the initial version of its enterprise architecture in September 2003. In August 2004 we reported that the department's initial enterprise architecture provided a partial basis upon which to build future versions but was missing most of the content necessary to be considered a well-defined architecture. In particular, the content of this initial version was not systematically derived from a DHS or national corporate business strategy; rather, it was more the result of an amalgamation of the existing architectures that several of DHS's predecessor agencies already had. To its credit, the department recognized the limitations of the initial architecture. To assist DHS in evolving its architecture, we recommended 41 actions aimed at having DHS add needed architecture content. Since then, the department reported that it had taken steps in response to our recommendations. For example, DHS issued version 2 of its enterprise architecture, which the department reported contained additional business/mission, service, and technical descriptions, in October 2004. Subsequently, DHS decided to issue annual architecture updates. The first of these, DHS EA 2006, was issued in March 2006. In May 2007 we reported that DHS EA 2006 partially addresses the content shortcomings in earlier versions. However, the full depth and breadth of architecture content that our 41 recommendations provided for is not reflected. For example, we recommended that DHS use, among other things, an analysis of the gaps between the current ("as-is") and future ("to-be") states of the architecture to define missing and needed capabilities and form the basis for its transition plan. However, DHS EA 2006 does not include a transition plan and it does not include any evidence of a gap analysis. In addition we reported in August 2006 on DHS's enterprise architecture management capability, stating, among other things, that DHS has not fully implemented 7 of 31 elements of our Enterprise Architecture Management Maturity Framework. For example, we found that the department's enterprise architecture products and management processes do not undergo independent verification and validation and that the return on enterprise architecture investment is not measured and reported. For more information, see *Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains,* GAO-04-777; GAO-06-598T; *Homeland Security: DHS Enterprise Architecture Continues to Evolve but Improvements Needed,* GAO-07-564; *Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation,* GAO-06-831; and *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1),* GAO-03-584G.<br>*DHS updated information:* In March 2007, DHS reported that it has already addressed, or has identified tasks in its program plan to address, those elements of our Enterprise Architecture Management Maturity Framework that we found that the department had previously not fully or partially satisfied. In June 2007, DHS provided us with a newer, more current version of its architecture (i.e., DHS EA 2007), which it reports addresses many of our prior concerns.<br>*Our assessment:* Because of the considerable time and resources necessary to evaluate an architecture as large and complex as DHS's, we have not had an opportunity to assess this latest version. | No assessment made |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 6. Implement a comprehensive enterprise architecture | *GAO findings:* Between 2003 and 2007, we have reported on the extent to which the department has implemented its enterprise architecture to ensure alignment of major information technology investments, such as US-VISIT, CBP's Automated Commercial Environment system, and ICE's Atlas program. We reported in September 2003 that US-VISIT was making assumptions and decisions about the program because the operational context was unsettled and unclear. In February 2005 we reported that DHS had assessed US-VISIT for alignment with the business and information/data views of its architecture and found it to be in compliance. However, the assessment did not include other architecture views, and DHS could not provide us with sufficient documentation to understand its architecture compliance methodology and criteria, or verifiable analysis to justify its determination. In February 2007, we reported that DHS had not reviewed US-VISIT architecture compliance for more than 2 years, during which time both US-VISIT and the DHS enterprise architecture had changed. We also reported in March 2005 and again in May 2006 that DHS's determination that the Automated Commercial Environment was aligned with DHS's architecture was not supported by sufficient documentation to allow us to understand its architecture compliance methodology and criteria or with verifiable analysis demonstrating alignment. We reported in September 2005 and again in July 2006 that DHS had determined that Atlas was in compliance with the architecture but that this determination was also not based on a documented analysis or methodology that is necessary to make such a determination. In August 2006 we reported on DHS's enterprise architecture management capability. Among other things, we found that although DHS had a process that required information technology investment compliance with its enterprise architecture, the process did not include a methodology with detailed compliance criteria. For more information, see *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed,* GAO-03-1083; *Homeland Security: Some Progress Made, but Many Challenges Remain on U.S. Visitor and Immigrant Status Indicator Technology Program,* GAO-05-202; *Homeland Security: Planned Expenditures for U.S. Visitor and Immigrant Status Program Need to Be Adequately Defined and Justified,* GAO-07-278; *Information Technology: Customs Automated Commercial Environment Progress Progressing, but Need for Management Improvements Continues,* GAO-05-267; *Information Technology: Customs Has Made Progress on Automated Commercial Environment System, but It Faces Long-Standing Management Challenges and New Risks,* GAO-06-580; *Information Technology: Management Improvements Needed on Immigration and Customs Enforcement's Infrastructure Modernization Program,* GAO-05-805; *Information Technology: Immigration and Customs Enforcement Is Beginning to Address Infrastructure Modernization Program Weaknesses but Key Improvements Still Needed,* GAO-06-823; GAO-03-584G; and GAO-06-831.<br>*DHS updated information:* DHS did not provide us with updated information on its efforts to implement an enterprise architecture.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. We have reported that major DHS information technology investments have not been fully aligned with DHS's enterprise architecture, and DHS did not provide us evidence that these investments and others have been fully aligned with DHS's enterprise architecture. | Generally not achieved |
| 7. Develop a process to effectively manage information technology investments | *GAO findings:* DHS has not fully developed a process to manage information technology investments. Specifically, in April 2007, we reported that DHS has established the management structure to effectively manage its investments. However, the department had yet to fully define 8 of the 11 related policies and procedures defined by our information technology investment management framework.[a] Specifically, while DHS had documented the policies and related procedures for project-level management, some of these procedures did not include key elements. For example, procedures for selecting investments did not cite either the specific criteria or steps for prioritizing and selecting new information technology proposals, and procedures for management oversight of information technology projects and systems did not specify the rules that the investment boards were to follow in overseeing | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | investments. In addition, the department had yet to define most of the policies associated with managing its information technology projects as investment portfolios. Officials attributed the absence of project-level procedures to resource constraints, stating that with a full time staff of six to support departmentwide investment management activities, they were more focused on performing investment management rather than documenting it in great detail. They attributed the absence of policies and procedures at the portfolio level to other investment management priorities. For more information, see *Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments,* GAO-07-424.<br>*DHS updated information:* In March and April 2007, DHS provided us with information on its efforts to develop a process to effectively manage information technology investments. In particular, DHS reported that while it has substantial room for improvement in this area, DHS has developed an investment oversight foundation that can be effective.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has taken some actions to develop a process to effectively manage information technology investments, but much work remains. Specifically, the department has not yet fully defined many of the key policies and procedures identified in our information technology investment management framework. | |
| 8. Implement a process to effectively manage information technology investments | *GAO findings:* DHS is not effectively managing its information technology investments. Specifically, in April 2007, we reported that DHS had not fully implemented any of the key practices our information technology investment management framework specifies as being needed to actually control investments—either at the project level or at the portfolio level. For example, according to DHS officials and the department's control review schedule, the investment boards had not conducted regular reviews of investments. Further, while control activities were sometimes performed, they were not performed consistently across all information technology projects. In addition, because the policies and procedures for portfolio management had yet to be defined, control of the department's investment portfolios was ad hoc, according to DHS officials. To strengthen information technology investment management, officials told us that they had hired a portfolio manager and were recruiting another one. For more information, see GAO-07-424.<br>*DHS updated information:* In March 2007, DHS provided us with information on its efforts to develop a process to effectively manage information technology investments. In particular, DHS reported that while it has substantial room for improvement in this area, DHS has developed an investment oversight foundation that can be effective.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has taken some actions to implement a process to effectively manage information technology investments, but more work remains, particularly in implementing the key practices of our information technology investment management framework for actually controlling investments. | Generally not achieved |
| 9. Develop policies and procedures for effective information systems development and acquisition | *GAO findings:* In March 2006, we reported that DHS was in the process of drafting policies and procedures to establish a departmentwide systems development life cycle methodology that was intended to provide a common management approach to systems development and acquisition. According to DHS, the goals of the systems development life cycle are to help align projects to mission and business needs and requirements; incorporate accepted industry and government standards, best practices, and disciplined engineering methods, including information technology maturity model concepts; ensure that formal reviews and approval required by the process are consistent with DHS's investment management process; and institute disciplined life cycle management practices, including planning and evaluation in each phase of the information system cycle. The methodology is to apply to DHS's information technology portfolio as well as other capital asset acquisitions. Under the methodology, each program is expected to, among other things, follow disciplined project planning and management processes balanced by effective management controls; have a comprehensive | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | project management plan; base project plans on user requirements that are testable, and traceable to the work products produced; and integrate information security activities throughout the systems development life cycle. For more information, see GAO-06-598T.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to develop policies and procedures for information systems development and acquisition. Specifically, DHS's March 2007 Information Technology Integration and Management directive notes that the DHS Chief Information Officer is responsible for reviewing and approving any information technology acquisition in excess of $2.5 million.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation, as the life cycle methodology for managing systems development and acquisition in still in draft form and each component has its own methodology. | |
| 10. Implement policies and procedures for effective information systems development and acquisition | *GAO findings:* DHS has faced challenges in implementing policies and procedures for effective information systems development and acquisition. Specifically, our reviews of several key (nonfinancial) information technology programs (e.g., US-VISIT, CBP's Automated Commercial Environment, and ICE's Atlas program) have disclosed numerous weaknesses in the implementation of policies and procedures relating to key development and acquisition areas, such as requirements development and management, test management, project planning, validation and verification, and contract management oversight. We have ongoing work related to specific systems acquisition programs. For more information, see GAO-04-702.<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to develop policies and procedures for information systems development and acquisition. Specifically, DHS's March 2007 Information Technology Integration and Management directive notes that the DHS Chief Information Officer is responsible for reviewing and approving any information technology acquisition in excess of $2.5 million and to ensure the alignment of the department's purchases with the target enterprise architecture.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. DHS has taken some actions to develop policies and procedures for reviewing information technology acquisitions. However, DHS did not provide us with evidence that these policies and procedures have been effectively implemented with regard to specific information technology acquisition programs, such as US-VISIT and the Automated Commercial Environment. | Generally not achieved |
| 11. Provide operational capabilities for information technology infrastructure and applications | *GAO findings and assessment:* We have not completed work in this area upon which to make an assessment. We previously reported that a gauge of DHS's progress in managing its information technology investments is the extent to which it has deployed and is currently operating more modern information technology systems and infrastructure. | No assessment made |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 12. Develop policies and procedures to ensure protection of sensitive information | *GAO findings and assessment:* We conclude that DHS has generally achieved this performance expectation, as DHS has developed policies and procedures for protecting sensitive information. The Chief Information Officer designated the Chief Information Security Officer to carry out specific information security responsibilities that include developing and maintaining a departmentwide information security program; developing departmental information security policies and procedures; providing the direction and guidance necessary to ensure that information security throughout the department is compliant with federal information security requirements and policies; and advising the Chief Information Officer on the status and issues involving security aspects of the departmentwide information security program. Since DHS became operational in March 2003, the Chief Information Security Officer has developed and documented departmental policies and procedures that could provide a framework for implementing an agencywide information security program. For more information, see *Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program,* GAO-05-700. | Generally achieved |
| 13. Implement policies and procedures to effectively safeguard sensitive information | *GAO and DHS IG findings:* DHS has not yet implemented policies and procedures for safeguarding sensitive information. In June 2005, we reported that DHS had yet to effectively implement a comprehensive, departmentwide information security program to protect the information and information systems that support its operations and assets. In particular, although it had developed and documented departmental policies and procedures that could provide a framework for implementing such a program, certain departmental components had not yet fully implemented key information security practices and controls. Examples of weaknesses in components' implementation included incomplete or missing elements in risk assessments, security plans, and remedial action plans, as well as incomplete, nonexistent, or untested continuity of operations plans. In September 2006, the DHS IG reported that DHS had made progress in implementing its information security program. For example, the DHS IG found that DHS had taken measures to develop a process to maintain a comprehensive systems inventory and to increase the number of operational systems that had been certified and accredited. Despite several improvements in DHS's information security program, the DHS IG found that DHS components, through their Information Systems Security Managers, had not completely aligned their respective information security programs with DHS's overall policies, procedures, and practices. For example, all DHS systems had not been properly certified and accredited; all components' information security weaknesses were not included in a plan of action and milestones; data in the enterprise management tool, Trusted Agent FISMA, was not complete or current; and system contingency plans had not been tested for all systems. The DHS IG reported that while DHS had issued substantial guidance designed to create and maintain secure systems, there were areas where the implementation of agencywide information security procedures required strengthening: (1) certification and accreditation; (2) plan of action and milestones; (3) security configurations; (4) vulnerability testing and remediation; (5) contingency plan testing; (6) incident detection, analysis, and reporting; and (7) specialized security training. For more information, see GAO-06-598T and GAO-05-700. Also, see Department of Homeland Security Office of Inspector General, *Evaluation of DHS' Information Security Program for Fiscal Year 2006,* OIG-06-62 (Washington, D.C.: September 2006).<br>*DHS updated information:* In March 2007, DHS provided us with updated information on its efforts to implement policies and procedures to safeguard sensitive information. DHS reported initiating an Information Technology Security Remediation Project in 2006 to ensure that all DHS components implemented a common set of information security practices and key controls at the system level. According to DHS, all system owners were required to implement a common set of baseline controls as outlined in the directive on DHS Information Security Policy and to demonstrate compliance by submitting appropriate system security documentation, including a risk assessment, a system security plan, results of controls testing, a contingency plan (if required), and an accreditation letter signed by an appropriate | Generally not achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| | Designated Accrediting Authority, for a department-level review. By the end of October 2006, DHS reported that 95 percent of the department's information technology systems were fully accredited.<br>*Our assessment:* We conclude that DHS has generally not achieved this performance expectation. Although DHS has taken actions to implement policies and procedures to safeguard sensitive information, it has not yet effectively done so. For example, the DHS IG reported that the department had a material weaknesses in the effectiveness of general and application controls over its financial systems, and our ongoing work has identified significant information security weaknesses that pervade systems supporting a key departmental program. In addition, while DHS has taken actions to ensure that certification and accreditation activities are completed, the department did not provide evidence that it has strengthened its incident detection, analysis, and reporting and testing activities. | |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

[a] GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity,* GAO-04-394G (Washington, D.C.: March 2004).

## DHS Has Made Moderate Progress in Real Property Management

DHS has taken actions to implement its real property management responsibilities. Key elements of real property management, as specified in Executive Order 13327, "Federal Real Property Asset Management," include establishment of a Senior Real Property Officer, development of an asset inventory, and development and implementation of an asset management plan and performance measures. In June 2006, the Office of Management and Budget upgraded DHS's Real Property Asset Management Score from red to yellow after DHS developed an approved Asset Management Plan, developed a generally complete real property data inventory, submitted this inventory for inclusion in the governmentwide real property inventory database, and established performance measures consistent with Federal Real Property Council standards. DHS also designated a Senior Real Property Officer as directed by Executive Order 13327.

As shown in table 42, we identified nine performance expectations for DHS in the area of real property management and found that overall DHS has made moderate progress in meeting those expectations. Specifically, we found that DHS has generally achieved six of the expectations and has generally not achieved three others. Our assessments for real property management are based on a report on DHS's real property management released in June 2007.

Table 42: Performance Expectations and Progress Made in Real Property Management

| Performance expectation | Assessment | | |
|---|---|---|---|
| | Generally achieved | Generally not achieved | No assessment made |
| 1. Establish a Senior Real Property Officer who actively serves on the Federal Real Property Council | ✓ | | |
| 2. Complete and maintain a comprehensive inventory and profile of agency real property | ✓ | | |
| 3. Provide timely and accurate information for inclusion in the governmentwide real property inventory database | ✓ | | |
| 4. Develop an Office of Management and Budget-approved asset management plan | ✓ | | |
| 5. Establish an Office of Management and Budget-approved 3-year rolling timeline with certain deadlines by which the agency will address opportunities and determine its priorities as identified in the asset management plan | ✓ | | |
| 6. Demonstrate steps taken toward implementation of the asset management plan | | ✓ | |
| 7. Establish real property performance measures | ✓ | | |
| 8. Use accurate and current asset inventory information and real property performance measures in management decision making | | ✓ | |
| 9. Ensure the management of agency property assets is consistent with the agency's overall strategic plan, the agency asset management plan, and the performance measures | | ✓ | |
| **Total** | **6** | **3** | **0** |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

Table 43 provides more detailed information on the progress that DHS has made in taking actions to achieve each performance expectation in the area of real property management and our assessment of whether DHS has taken steps to satisfy most of the key elements of the performance expectation (generally achieved) or has not taken steps to satisfy most of the performance expectation's key elements (generally not achieved).

**Table 43: Performance Expectations and Assessment of DHS Progress in Real Property Management**

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 1. Establish a Senior Real Property Officer who actively serves on the Federal Real Property Council | *GAO findings and assessment:* DHS has appointed a Senior Real Property Officer whose official title is Chief Administrative Officer. The Senior Real Property Officer serves on the Federal Real Property Council and coordinates the formulation and implementation of real property management planning for DHS. For more information, see *Federal Real Property: DHS Has Made Progress, but Additional Actions Are Needed to Address Real Property Management and Security Challenges*, GAO-07-658. | Generally achieved |
| 2. Complete and maintain a comprehensive inventory and profile of agency real property | *GAO findings and assessment:* DHS has developed and maintained an inventory of agency real property. DHS's real property data inventory, called the Real Property Information System, is designed to enable active and efficient stewardship of its real property assets. It has been in place since April 2006. For more information, see GAO-07-658. | Generally achieved |
| 3. Provide timely and accurate information for inclusion in the governmentwide real property inventory database | *GAO findings and assessment:* DHS submits data on real property that it owns and directly leases to the General Services Administration's governmentwide real property inventory. For more information, see GAO-07-658. | Generally achieved |
| 4. Develop an Office of Management and Budget-approved asset management plan | *GAO findings and assessment:* DHS has developed an Office of Management and Budget-approved asset management plan. The administration's Real Property Initiative required DHS to develop and implement an asset management plan, develop a real property inventory that tracked DHS's assets, and develop and use performance measures. The Office of Management and Budget approved DHS's asset management plan in June 2006. For more information, see GAO-07-658. | Generally achieved |
| 5. Establish an Office of Management and Budget-approved 3-year rolling timeline with certain deadlines by which the agency will address opportunities and determine its priorities as identified in the asset management plan | *GAO findings and assessment:* DHS has developed an Office of Management and Budget-approved 3-year timeline to implement the goals and objectives of the asset management plan. For more information, see GAO-07-658. | Generally achieved |
| 6. Demonstrate steps taken toward implementation of the asset management plan | *GAO findings and assessment:* DHS has yet to demonstrate full implementation of its asset management plan. For more information, see GAO-07-658. | Generally not achieved |
| 7. Establish real property performance measures | *GAO findings and assessment:* DHS has established asset management performance measures, including facility condition, utilization, mission dependency, and annual operating and maintenance costs. For more information, see GAO-07-658. | Generally achieved |

| Performance expectation | Summary of findings | Assessment |
|---|---|---|
| 8. Use accurate and current asset inventory information and real property performance measures in management decision making | *GAO findings and assessment:* DHS has yet to demonstrate full use of asset inventory information and performance measures in management decision making. For more information, see GAO-07-658. | Generally not achieved |
| 9. Ensure the management of agency property assets is consistent with the agency's overall strategic plan, the agency asset management plan, and the performance measures | *GAO findings and assessment:* DHS has not yet taken steps to ensure that the management of agency property assets is consistent with the DHS strategic plan, asset management plan, and performance measures. For more information, see GAO-07-658. | Generally not achieved |

Source: GAO analysis.

Note: An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation. However, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, "generally not achieved" indicates that DHS has not yet taken sufficient actions to satisfy most elements of the performance expectation. An assessment of "generally not achieved" may be warranted even where DHS has put forth substantial effort to satisfy some but not most elements of an expectation. In cases when we or the DHS IG have not completed work upon which to base an assessment of DHS actions to satisfy a performance expectation, and/or the information DHS provided did not enable us to clearly determine the extent to which DHS has achieved the performance expectation, we indicated "no assessment made."

## Cross-cutting Issues Have Hindered DHS's Implementation Efforts

Our work has identified homeland security challenges that cut across DHS's mission and core management functions. These issues have impeded the department's progress since its inception and will continue as DHS moves forward. While it is important that DHS continue to work to strengthen each of its mission and core management functions, it is equally important that these key issues be addressed from a comprehensive, departmentwide perspective to help ensure that the department has the structure and processes in place to effectively address the threats and vulnerabilities that face the nation. These issues include: (1) transforming and integrating DHS's management functions; (2) establishing baseline performance goals and measures and engaging in effective strategic planning efforts; (3) applying and improving a risk management approach for implementing missions and making resource allocation decisions; (4) sharing information with key stakeholders; and (5) coordinating and partnering with federal, state, local, and private sector agencies. We have made numerous recommendations to DHS to strengthen these efforts, and the department has made progress in implementing some of these recommendations.

## DHS Has Not Yet Transformed Its Component Agencies into a Fully Functioning Department

DHS has faced a variety of difficulties in its efforts to transform into a fully functioning department, and we have designated DHS implementation and transformation as high-risk. We first designated DHS's implementation and transformation as high-risk in 2003 because 22 disparate agencies had to transform into one department. Many of these individual agencies were facing their own management and mission challenges. But most importantly, the failure to effectively address DHS's management challenges and program risks could have serious consequences for our homeland security as well as our economy. We kept DHS implementation and transformation on the high-risk list in 2005 because serious transformation challenges continued to hinder DHS's success. Since then, our and the DHS IG's reports have documented DHS's progress and remaining challenges in transforming into an effective, integrated organization. For example, in the management area, DHS has developed a strategic plan, is working to integrate some management functions, and has continued to form necessary partnerships to achieve mission success. Despite these efforts, we reported that DHS implementation and transformation remains on the 2007 high-risk list because numerous management challenges remain, such as in the areas of acquisition, financial, human capital, and information technology management. We stated that the array of management and programmatic challenges continues to limit DHS's ability to carry out its roles under the *National Strategy for Homeland Security* in an effective risk-based way.

We have recommended that agencies on the high-risk produce a corrective action plan that defines the root causes of identified problems, identifies effective solutions to those problems, and provides for substantially completing corrective measures in the near term. Such a plan should include performance metrics and milestones, as well as mechanisms to monitor progress. In the spring of 2006, DHS provided us with a draft corrective action plan that did not contain key elements we have identified as necessary for an effective corrective action plan, including specific actions to address identified objectives. As of May 2007, DHS had not submitted a corrective action plan to the Office of Management and Budget. According to the Office of Management and Budget, this is one of the few high-risk areas that has not produced a final corrective action plan.

Our prior work on mergers and acquisitions, undertaken before the creation of DHS, found that successful transformations of large organizations, even those faced with less strenuous reorganizations than DHS, can take at least 5 to 7 years to achieve. We reported that the creation of DHS is an enormous management challenge and that DHS faces a formidable task in its transformation efforts as it works to integrate over 170,000 federal employees from 22 component agencies. Each component agency brought differing missions, cultures, systems, and procedures that the new department had to efficiently and effectively integrate into a single, functioning unit. At the same time it weathers these growing pains, DHS must still fulfill its various homeland security and other missions.

To strengthen its transformation efforts, we recommended, and DHS agreed, that it should develop an overarching management integration strategy, and provide the then DHS Business Transformation Office with the authority and responsibility to serve as a dedicated integration team and also to help develop and implement the strategy. We reported that although DHS has issued guidance and plans to assist management integration on a function by function basis, it has not developed a plan that clearly identifies the critical links that should occur across these functions, the necessary timing to make these links occur, how these interrelationships will occur, and who will drive and manage them. In addition, although DHS had established a Business Transformation Office that reported to the Under Secretary for Management to help monitor and look for interdependencies among the individual functional management integration efforts, that office was not responsible for leading and managing the coordination and integration itself. We understand that the Business Transformation Office has been recently eliminated. We have suggested that Congress should continue to monitor whether it needs to provide additional leadership authorities to the DHS Under Secretary for Management, or create a Chief Operating Officer/Chief Management Officer position which could help elevate, integrate, and institutionalize DHS's management initiatives. The Implementing Recommendations of the 9/11 Commission Act of 2007, enacted in August 2007, designates the Under Secretary for Management as the Chief Management Officer and principal advisor on management-related matters to the Secretary.[28] Under the Act, the Under Secretary is responsible for developing a transition and succession plan for the incoming Secretary and Under Secretary to guide the transition of management functions to a new administration. The Act further authorizes the incumbent Under Secretary as of November 8, 2008 (after the next presidential election), to remain in the position until a

[28] Implemented Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 2405, 121 Stat. 266 (2007).

successor is confirmed to ensure continuity in the management functions of DHS.

In addition, transparency plays an important role in helping to ensure efficient and effective transformation efforts. With regard to DHS, we have reported that DHS has not made its management or operational decisions transparent enough so that Congress can be sure it is effectively, efficiently, and economically using the billions of dollars in funding it receives annually. More specifically, in April 2007, we testified that we have encountered access issues in numerous engagements, and the lengths of delay have been both varied and significant and have affected our ability to do our work in a timely manner. We reported that we have experienced delays with DHS components that include CBP, ICE, FEMA, and TSA on different types of work such as information sharing, immigration, emergency preparedness in primary and secondary schools, and accounting systems. The Secretary of DHS and the Under Secretary for Management have stated their desire to work with us to resolve access issues and to provide greater transparency. It will be important for DHS to become more transparent and minimize recurring delays in providing access to information on its programs and operations so that Congress, GAO, and others can independently assess its efforts.

## DHS Has Not Yet Developed Outcome-Based Measures to Assess Strategic Performance in Many Areas

DHS has not always implemented effective strategic planning efforts and has not yet fully developed performance measures or put into place structures to help ensure that the agency is managing for results. We have identified strategic planning as one of the critical success factors for new organizations. This is particularly true for DHS, given the breadth of its responsibility and need to clearly identify how stakeholders' responsibilities and activities align to address homeland security efforts. The Government Performance and Results Act (GPRA) of 1993 requires that federal agencies consult with the Congress and key stakeholders to assess their missions, long-term goals, strategies, and resources needed to achieve their goals. It also requires that the agency include six key components in its strategic plan: (1) a mission statement; (2) long-term goals and objectives; (3) approaches (or strategies) to achieve the goals and objectives; (4) a description of the relationship between annual and long-term performance goals; (5) key factors that could significantly affect achievement of the strategic goals; and (6) a description of how program evaluations were used to establish or revise strategic goals. Other best practices in strategic planning and results management that we have identified include involving stakeholders in the strategic planning process, continuously monitoring internal and external environments to anticipate future challenges and avoid potential crises, holding managers accountable for the results of their programs, and aligning program performance measures and individual performance expectations at each organizational level with agencywide goals and objectives.

DHS issued a departmentwide strategic plan in 2004 that addressed five of six GPRA-required elements. The plan included a mission statement, long-term goals, strategies to achieve the goals, key external factors, and program evaluations, but did not describe the relationship between annual and long-term goals. The linkage between annual and long-term goals is important for determining whether an agency has a clear sense of how it will assess progress toward achieving the intended results of its long-term goals. While DHS's Performance Budget Overview and other documents include a description of the relationship between annual and long-term goals, not including this in the strategic plan made it more difficult for DHS officials and stakeholders to identify how their roles and responsibilities contributed to DHS's mission. In addition, although DHS's planning documents described programs requiring stakeholder coordination to effectively implement them, stakeholder involvement in the planning process itself was limited. Given the many other organizations at all levels of government and in the private sector whose involvement is key to meeting homeland security goals, earlier and more comprehensive stakeholder involvement in the planning process is essential to the success of DHS's planning efforts. Such involvement is important to ensure that stakeholders help identify and agree on how their daily operations and activities contribute to fulfilling DHS's mission. To make DHS a more results-oriented agency, we recommended that DHS's strategic planning process include direct consultation with external stakeholders, that its next strategic plan include a description of the relationship between annual performance goals and long-term goals, and that the next strategic plan adopt additional good strategic planning practices, such as ensuring that the strategic plan includes a timeline for achieving long-terms goals and a description of the specific budgetary, human capital, and other resources needed to achieve those goals. According to DHS officials, the department is planning to issue an updated strategic plan, but they did not provide a target time frame for when the plan would be issued.

We have also reported on the importance of the development of outcome-based performance goals and measures as part of strategic planning and results management efforts. Performance goals and measures are intended to provide Congress and agency management with information to systematically assess a program's strengths, weaknesses, and performance. A performance goal is the target level of performance expressed as a tangible, measurable objective against which actual achievement will be compared. A performance measure can be defined as an indicator, statistic, or metric used to gauge program performance. Outcome-oriented measures show results or outcomes related to an initiative or program in terms of its effectiveness, efficiency, or impact.[29]

A number of DHS's programs lack outcome goals and measures, which may hinder the department's ability to effectively assess the results of program efforts or fully assess whether the department is using resources effectively and efficiently, especially given various agency priorities for resources. In particular, we have reported that some of DHS's components have not developed adequate outcome-based performance measures or comprehensive plans to monitor, assess, and independently evaluate the effectiveness of their plans and performance. For example, in August 2005 we reported that ICE lacked outcome goals and measures for its worksite enforcement program and recommended that the agency set specific time frames for developing these goals and measures. In March 2006, we reported that USCIS had not yet established performance goals and measures to assess its benefit fraud activities, and we recommended that they do so. Further, we have also reported that many of DHS's border-related performance goals and measures are not fully defined or adequately aligned with one another, and some performance targets are not realistic. Yet, we have also recognized that DHS faces some inherent difficulties in developing performance goals and measures to address its unique mission and programs, such as in developing measures for the effectiveness of its efforts to prevent and deter terrorist attacks.

## DHS Has Not Fully Applied a Risk Management Approach in Implementing All Mission Areas

DHS has not fully adopted and applied a risk management approach in implementing its mission and core management functions. Risk management has been widely supported by the President and Congress as a management approach for homeland security, and the Secretary of Homeland Security has made it the centerpiece of departmental policy. We have previously reported that defining an acceptable, achievable (within

[29] The performance expectations we identified for DHS in this report do not represent performance goals or measures for the department. We define performance expectations as a composite of the responsibilities or functions, derived from legislation, homeland security presidential directives and executive orders, DHS planning documents, and other sources, that the department is to address in implementing efforts in its mission and management areas.

constrained budgets) level of risk is an imperative to address current and future threats. Many have pointed out, as did the Gilmore and 9/11 Commissions, that the nation will never be completely safe and total security is an unachievable goal. Within its sphere of responsibility, DHS cannot afford to protect everything against all possible threats. As a result, DHS must make choices about how to allocate its scarce resources to most effectively manage risk. A risk management approach can help DHS make decisions systematically and is consistent with the *National Strategy for Homeland Security* and DHS's strategic plan, which have called for the use of risk-based decisions to prioritize DHS's resource investments regarding homeland security related programs.

Several DHS component agencies have taken steps toward integrating risk-based decision making into their decision making processes. For example, the Coast Guard has taken actions to mitigate vulnerabilities and enhance maritime security. Security plans for seaports, facilities, and vessels have been developed based on assessments that identify their vulnerabilities. In addition, the Coast Guard used a Maritime Security Risk Assessment Model to prioritize risk according to a combination of possible threat, consequence, and vulnerability scenarios. Under this approach, seaport infrastructure that was determined to be both a critical asset and a likely and vulnerable target would be a high priority for funding security enhancements. By comparison, infrastructure that was vulnerable to attack but not as critical or infrastructure that was very critical but already well protected would be lower in priority. In the transportation area, TSA has incorporated risk-based decision-making into number of its programs and processes. For example, TSA has started to incorporate risk management principles into securing air cargo, but has not conducted assessments of air cargo vulnerabilities or critical assets (cargo facilities and aircraft)—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. TSA also completed an Air Cargo Strategic Plan in November 2003 that outlined a threat-based risk management approach to securing the nation's air cargo transportation system. However, TSA's existing tools for assessing vulnerability have not been adapted for use in conducting air cargo assessments, nor has TSA established a schedule for when these tools would be ready for use.

Although some DHS components have taken steps to apply risk-based decision making in implementing their mission functions, we also found that other components have not always utilized such an approach. DHS has not performed comprehensive risk assessments in transportation, critical infrastructure, and the immigration and customs systems to guide resource allocation decisions. For example, DHS has not fully utilized a risk-based strategy to allocate resources among transportation sectors. Although TSA has developed tools and processes to assess risk within and across transportation modes, it has not fully implemented these efforts to drive resource allocation decisions. We also recently identified concerns about DHS's use of risk management in distributing grants to states and localities. 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 Urban Areas Security Initiative 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. However, we found 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, affect 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 for fiscal year 2006. DHS leadership could make more informed policy decisions if it were provided with alternative risk estimates and funding allocations resulting from analyses of varying data, judgments, and assumptions. We also reported that DHS has not applied a risk management approach in deciding whether and how to invest in specific capabilities for a catastrophic threat, and we recommended that it do so.

In April 2007, DHS established the new Office of Risk Management and Analysis to serve as the DHS Executive Agent for national-level risk management analysis standards and metrics; develop a standardized approach to risk; develop an approach to risk management to help DHS leverage and integrate risk expertise across components and external stakeholders; assess DHS risk performance to ensure programs are measurably reducing risk; and communicating DHS risk management in a manner that reinforces the risk-based approach. According to DHS, the office's activities are intended to develop a risk architecture, with standardized methodologies for risk analysis and management, to assist in the prioritization of risk reduction programs and to ensure that DHS component risk programs are synchronized, integrated, and use a common approach. Although this new office should help to coordinate risk management planning and activities across the department, it is too early to tell what effect this office will have on strengthening departmentwide risk management activities.

## Information Sharing Remains a Challenge for DHS

The federal government, including DHS, has made progress in developing a framework to support a more unified effort to secure the homeland, including information sharing. However, opportunities exist to enhance the effectiveness of information sharing among federal agencies and with state and local governments and private sector entities. As we reported in August 2003, efforts to improve intelligence and information sharing needed to be strengthened. In 2005, we designated information sharing for homeland security as high-risk. We recently reported that the nation still lacked an implemented set of governmentwide policies and processes for sharing terrorism information, but has issued a strategy on how it will put in place the overall framework, policies, and architecture for sharing with all critical partners—actions that we and others have recommended. The Intelligence Reform and Terrorism Prevention Act of 2004 required that the President create an "information sharing environment" to facilitate the sharing of terrorism information, yet this environment remains in the planning stage. An implementation plan for the environment, which was released on November 16, 2006, defines key tasks and milestones for developing the information sharing environment, including identifying barriers and ways to resolve them, as we recommended. We noted that completing the information sharing environment is a complex task that will take multiple years and long-term administration and congressional support and oversight, and will pose cultural, operational, and technical challenges that will require a collaborated response.

DHS has taken some steps to implement its information sharing responsibilities. For example, DHS implemented a system to share homeland security information. States and localities are also creating their own information "fusion" centers, some with DHS support. DHS has further implemented a program to protect sensitive information the private sector provides it on security at critical infrastructure assets, such as nuclear and chemical facilities. However, the DHS IG found that users of the information system were confused with it and as a result did not regularly use it; and DHS had not secured of the private sector's trust that the agency could adequately protect and effectively use the information that sector provided. These challenges will require longer-term actions to resolve. Our past work in the information sharing and warning areas has highlighted a number of other challenges that need to be addressed. These challenges include developing productive information sharing relationships among the federal government, state and local governments, and the private sector; and ensuring that the private sector receives better information on potential threats.

## DHS Has Faced Difficulties in Coordinating with Homeland Security Partners

In addition to providing federal leadership with respect to homeland security, DHS also plays a large role in coordinating the activities of other federal, state, local, private sector, and international stakeholders, but has faced challenges in this regard. To secure the nation, DHS must form effective and sustained partnerships between legacy component agencies and also with a range of other entities, including other federal agencies, state and local governments, the private and nonprofit sectors, and international partners. We have reported that successful partnering and coordination involves collaborating and consulting with stakeholders to develop and agree on goals, strategies, and roles to achieve a common purpose; identify resource needs; establish a means to operate across agency boundaries, such as compatible procedures, measures, data, and systems; and agree upon and document mechanisms to monitor, evaluate, and report to the public on the results of joint efforts. We have found that the appropriate homeland security roles and responsibilities within and between the levels of government and with the private sector are evolving and need to be clarified.

The implementation of the *National Strategy for Homeland Security* further underscores the importance for DHS of partnering and coordination. For example, 33 of the strategy's 43 initiatives are required to be implemented by 3 or more federal agencies and the *National Strategy* identifies the private sector as a key homeland security partner. If these entities do not effectively coordinate their implementation activities, they may waste resources by creating ineffective and incompatible pieces of a larger security program. For example, because the private sector owns or operates 85 percent of the nation's critical infrastructure, DHS must partner with individual companies and sector organizations in order to protect vital national infrastructure, such as the nation's water supply, transportation systems and chemical facilities. In October 2006 we reported that all 17 critical infrastructure sectors established their respective government councils, and nearly all sectors initiated their voluntary private sector councils in response to the National Infrastructure Protection Plan. The councils, among other things, are to identify their most critical assets, assess the risks they face, and identify protective measures, in sector-specific plans that comply with DHS's National Infrastructure Protection Plan.

DHS has taken other important actions in developing partnerships and mechanisms for coordinating with homeland security partners. For example, DHS formed the National Cyber Response Coordination Group to coordinate the federal response to cyber incidents of national significance. It is a forum of national security, law enforcement, defense, intelligence, and other government agencies that coordinates intragovernmental and public/private preparedness and response to and recovery from national level cyber incidents and physical attacks that have significant cyber consequences. In the area of maritime security, DHS has also taken actions to partner with a variety of stakeholders. For example, the Coast Guard reported to us that as of June 2006, 35 sector command centers had been created and that these centers were the primary conduit for daily collaboration and coordination between the Coast Guard and its port partner agencies. We also found that through its Customs-Trade Partnership Against Terrorism Program, CBP has worked in partnership with private companies to review their supply chain security plans to improve members' overall security.

However, DHS has faced some challenges in developing other effective partnerships and in clarifying the roles and responsibilities of various homeland security stakeholders. For example, in February 2007 we testified that because DHS has only limited authority to address security at chemical facilities it must continue to work with the chemical industry to ensure that it is assessing vulnerabilities and implementing security measures. Also, while TSA has taken steps to collaborate with federal and private sector stakeholders in the implementation of its Secure Flight program, in 2006 we reported these stakeholders stated that TSA has not provided them with the information they would need to support TSA's efforts as they move forward with the program. In addition, we reported in September 2005 that TSA did not effectively involve private sector stakeholders in its decision making process for developing security standards for passenger rail assets We recommended, and DHS developed, security standards that reflected industry best practices and could be measured, monitored, and enforced by TSA rail inspectors and, if appropriate, by rail asset owners. We have also made other recommendations to DHS to help strengthen its partnership efforts in the areas of transportation security and research and development.

Further, lack of clarity regarding roles and responsibilities caused DHS difficulties in coordinating with its emergency preparedness and response partners in responding to Hurricanes Katrina and Rita. For example, the Red Cross and FEMA had differing views about their roles and responsibilities under the National Response Plan, which hampered efforts to coordinate federal mass care assistance. Department of Labor and FEMA officials also disagreed about which agency was responsible for ensuring the safety and health of response and recovery workers. This lack of clarity about each other's roles and procedures resulted in delayed implementation of the National Response Plan's Worker Safety and Health Support Annex. We recommended that DHS take steps to improve partnering and coordination efforts as they relate to emergency preparedness and response, including to seek input from the state and local governments and private sector entities, such as the Red Cross, on the development and implementation of key capabilities, including those for interoperable communications.

## Concluding Observations

Given the dominant role that DHS plays in securing the homeland, it is critical that the department's mission programs and management systems and functions operate as efficiently and effectively as possible. In the more than 4 years since its establishment, the department has taken important actions to secure the border and the transportation sector and to defend against, prepare for, and respond to threats and disasters. DHS has had to undertake these critical missions while also working to transform itself into a fully functioning cabinet department—a difficult undertaking for any organization and one that can take, at a minimum, 5 to 7 years to complete even under less daunting circumstances. At the same time, a variety of factors, including Hurricanes Katrina and Rita, threats to and attacks on transportation systems in other countries, and new responsibilities and authorities provided by Congress have forced the department to reassess its priorities and reallocate resources to address key domestic and international events and to respond to emerging issues and threats.

As it moves forward, DHS will continue to face the challenges that have affected its operations thus far, including transforming into a high-performing, results-oriented agency; developing results-oriented goals and measures to effectively assess performance; developing and implementing a risk-based approach to guide resource decisions; and establishing effective frameworks and mechanisms for sharing information and coordinating with homeland security partners. DHS has undertaken efforts to address these challenges but will need to give continued attention to these efforts in order to efficiently and effectively identify and prioritize mission and management needs, implement efforts to address those needs, and allocate resources accordingly. Efforts to address these challenges will be especially important over the next several years given the threat environment and long-term fiscal imbalance facing the nation.

To address these challenges, DHS will need to continue its efforts to develop a results-oriented mission and management framework to guide implementation efforts and progress toward achieving desired outcomes. In moving forward, it will also be important for DHS to routinely reassess its mission and management goals, measures, and milestones to evaluate progress made, identify past and emerging obstacles, and examine alternatives to address those obstacles and effectively implement its missions. We have made nearly 700 recommendations to DHS on initiatives and reforms that would enhance its ability to implement its core mission and management functions, including developing performance goals and measures and setting milestones for key programs, making resource allocation decisions based on risk assessments, and developing and implementing internal controls to help ensure program effectiveness. DHS has generally agreed with our prior recommendations.

Moreover, taking those actions that we have suggested for agencies on our high-risk list provides a good road map for DHS as it works to further develop management structures that, once in place, could help the department more efficiently and effectively implement its mission and management functions. To be removed from our high-risk list, agencies first have to produce a corrective action plan that defines the root causes of identified problems, identifies effective solutions to those problems, and provides for substantially completing corrective measures in the near term. Such a plan should include performance metrics and milestones, as well as mechanisms to monitor progress. In the spring of 2006, DHS provided us with a draft corrective action plan that did not contain key elements we have identified as necessary for an effective corrective action plan, including specific actions to address identified objectives, and this plan has not yet been approved by the Office of Management and Budget. Second, agencies must demonstrate significant progress in addressing the problems identified in their corrective action plans. It will be important for DHS to become more transparent and minimize recurring delays in providing access to information on its programs and operations so that Congress, GAO, and others can independently assess its efforts. Finally, agencies, in particular top leadership, must demonstrate a commitment to sustain initial improvements in their performance over the long term. Although DHS leaders have expressed their intent to integrate legacy agencies into the new department, they have not dedicated the resources needed to oversee this effort.

A well-managed, high-performing Department of Homeland Security is essential to meeting the significant homeland security challenges facing the nation. As DHS continues to evolve, implement its programs, and integrate its functions, we will continue to review its progress and performance and provide information to Congress and the public on its efforts.

## Agency Comments and Our Evaluation

We requested comments on this report from the Secretary of Homeland Security. In comments dated July 20, 2007, and signed by the Undersecretary for Management (reprinted in their entirety in appendix II), DHS took issues with our methodology and disagreed with the conclusions we reached for 42 of the 171 performance expectations (specifically 41 of the 84 performance expectations where we assessed DHS as not having achieved the expectation and 1 of the 9 performance expectations for which we did not make an assessment). DHS also provided technical comments, which we considered and incorporated where appropriate.

DHS raised five general issues with our methodology. First, DHS believes that we altered the criteria by which we would judge the department's progress in changing our terminology from "generally addressed" to "generally achieved." As we communicated to DHS, we did not change the underlying assessment approach or evaluation criteria. Rather, we changed the way that we characterized DHS's progress for each performance expectation. For example, our definition for "generally addressed" and "generally achieved" did not change: "Our work has shown that DHS has taken steps to effectively satisfy the key elements of the performance expectation but may not have satisfied all of the elements." The change from "addressed" to "achieved" was not a change in methodology, criteria, or standards but only a change in language to better convey, in the context of results-oriented government, the legislative and executive intent behind these performance expectations that DHS achieve these expectations rather than merely begin to take steps that apply or are relevant to them.

Second, DHS took issue with the binary standard we used to assess each performance expectation. While we acknowledge the binary standard we applied is not perfect, we believe it is appropriate for this review because the administration generally has not established quantitative goals and measures for the performance expectations in connection with the various mission and management areas. Thus, we could not assess where along a spectrum of progress DHS stood for individual performance expectations. We chose the 2-step process for assessing DHS's progress—using a binary standard for individual performance expectations and a spectrum for broad mission and management areas—and fully disclosed it to and discussed it with DHS officials at the outset and throughout the review.

Third, DHS was concerned about how we defined our criteria for assessing DHS's progress in achieving each performance expectation and an apparent shift of criteria we applied after the department supplied us additional information and documents. With regard to how we defined our criteria and the performance expectations, the key elements for the expectations were inherent to each one, and we discussed these elements in each assessment. Further, we did not shift our criteria. Rather we employed a process by which we disclosed our preliminary analysis and assessments to DHS, received and analyzed additional documents and statements from DHS officials, and updated (and in many cases changed) our preliminary assessments based on the additional inputs. This process resulted in an improvement, a diminution, or no change in our assessment of the applicable area. In some cases, we added language to clarify the basis of our assessment after our review of the additional information DHS provided.

Fourth, DHS raised concerns that we did not "normalize" the application of our criteria by the many GAO analysts who had input to this review. Our methodology involved significant input by these analysts because they have had experience with the mission and management areas we were evaluating and were knowledgeable about the programs, specific performance expectations, activities, data, and results from each area. A core team of GAO analysts and managers reviewed all the inputs from these other GAO staff to ensure the consistent application of our methodology, criteria, and analytical process. In addition, our quality control process included detailed reviews of the facts included in this report, as well as assurance that we followed GAO's policies and generally accepted government auditing standards.

Finally, DHS points out that we treated all performance expectations as if they were of equal significance. In our scope and methodology section we recognize that qualitative differences between the performance expectations exist, but we did not apply a weight to the performance expectations because congressional, departmental, and other stakeholders' views on the relative priority of each performance expectation may be different and we did not believe it was appropriate to substitute our judgment for theirs.

DHS disagreed with our assessment of 42 of the 171 performance expectations—including 41 of the 84 performance expectations we assessed as generally not achieved—contending that we did not fully take account of all the actions it has taken relative to each expectation. Specifically, DHS believes that we expected DHS to achieve an entire expectation in cases where both DHS and we agree that ultimate achievement will not be possible for several more years, such as in the areas of border security and science and technology. This report provides Congress and the public with an assessment of DHS's progress as of July 2007 and does not reflect the extent to which DHS should have or could have made more progress. We believe that it is appropriate, after pointing out the expectation for a multiyear program and documenting the activities DHS has actually accomplished to date, to reach a conclusion about whether DHS had not implemented the program after 4 years.

DHS's concern that we have not adequately used or interpreted additional information it provided us, such as for performance expectations in the areas of aviation security and emergency preparedness and response, has little basis. We fully considered all information and documents DHS provided and described how we applied this information in the assessment portion of each performance expectation. In some cases DHS only provided us with testimonial information regarding its actions to achieve each performance expectation, but did not provide us with documentation verifying these actions. In the absence of such documentation to support DHS's claims, we concluded that DHS had generally not achieved the expectations. In other cases, the information and documents DHS provided did not convince us that DHS had generally achieved the performance expectation as stated or as we had interpreted it. In these cases, we explain the basis for our conclusions in the "GAO Assessment sections".Further, in some cases the information and documents DHS provided were not relevant to the specific performance expectation; in these situations we did not discuss them in our assessment. In addition, in some of its comments on individual performance expectations, DHS referenced new information that it did not provide to us during our review. In these cases we either explain our views on the information, or in one case we have changed our conclusion to "no assessment made".

Overall, we appreciate DHS's concerns and recognize that in a broad-based endeavor such as this, some level of disagreement is inevitable, especially at any given point in time.  However, we have been as transparent as possible regarding our purpose, methodology, and professional judgments. In table 44, we have summarized DHS's comments on the 42 performance expectations and our response to those comments.

**Table 44: Summary of DHS's Comments on 42 Performance Expectations and Our Response**

| Mission/<br>management area | Summary of DHS's comments and our response |
|---|---|
| **Border security** | *Performance expectation 4: Implement a program to detect and identify illegal border crossings between ports of entry*<br>*DHS's comments:* DHS commented that it is well on its way toward implementing the Secure Border Initiative, a comprehensive program to detect and identify illegal border crossings. DHS expressed concern that basing our assessment on the fact that SBI*net* has not been fully deployed is inconsistent with our acknowledgement in an exit conference that the Secure Border Initiative is "on a trajectory" towards achieving this comprehensive program. Further, DHS stated that our report's criticism of progress in implementing SBI*net* was surprising in light of our previous concern that SBI*net* was being implemented too quickly. DHS also expressed concern that we did not follow our ratings system because we said that progress that has been made on the implementation of SBI*net* is "unclear." In addition, DHS commented that our report does not consider DHS's efforts toward effective control over the northern border, and that contrary to the assertion that DHS will not begin work on the northern border until fiscal year 2009, CBP has tripled the number of agents assigned to the northern border since fiscal year 2001.<br>*Our response:* Although we recognize that DHS has made progress in implementing the Secure Border Initiative, SBI*net*, and other border security efforts to achieve this performance expectation, DHS data and our analysis showed that DHS has not yet achieved this expectation. For example, DHS data show that only about 392 miles or 6.5 percent of the 6,000 miles of U.S. land border were under effective control as of March 2007. Of these miles, only 12 miles are on the northern border. Further, we believe that assigning more Border Patrol agents to the northern border is only one part of the program DHS is implementing. Moreover, Border Patrol currently estimates that it apprehends less than half of the illegal alien traffic crossing our borders. We recognize that the Secure Border Initiative and SBI*net* are multiyear programs and are in the early stages of implementation and deployment, but we also noted that programs that predated the Secure Border Initiative faced challenges in implementation. Our work concluded that the risks to completing the program on time and within budget needed to be further reduced—not that program implementation needed to be delayed. |
| | *Performance expectation 6: Implement a strategy to detect and interdict illegal flows of cargo, drugs, and other items into the United States*<br>*DHS's comments:* DHS commented that our report makes reference to DHS's implementation efforts, but does not properly credit DHS for meeting this performance expectation. DHS stated that the Securing America's Borders at the Ports of Entry Strategic Plan defines a comprehensive national strategy and specifically outlines the department's efforts over the next 5 years to screen, detect, and interdict illegal cargo, contraband, weapons, agricultural products and other illicit substances. DHS reported that it has developed a formal Securing America's Borders at the Ports of Entry Implementation Plan and established the Securing America's Borders at the Ports of Entry Implementation Division to provide oversight and coordination in the execution of the strategic plan. DHS believes that it has set and successfully met several milestones related to this performance expectation in fiscal year 2006. Additionally, DHS stated that it has been working with federal, state, and local partners to develop a strategy and implementation plan which maximizes the efficiency of the resources that are dedicated to stopping the entry of illegal drugs into the United States along the southwest border. DHS commented that while our report acknowledges these counternarcotics efforts, it does not assign a proper assessment on the Counternarcotics Strategy and Implementation Plan solely because it has only recently been developed.<br>*Our response:* We fully reviewed and considered all of the information and documentation DHS provided to us and concluded that DHS has not yet generally achieved this performance expectation. DHS has made progress in implementing programs to achieve this performance expectation. However, our prior work identified challenges in implementation. Additionally, while we recognize that DHS has developed the Securing America's Borders at the Ports of Entry Strategic Plan and the related implementation plan and division, as well as the Counternarcotics Strategy and Implementation Plan, the actual implementation of these efforts are still in the early stages. Once implemented, they should help CBP detect and interdict illegal flows of goods into the United States. |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 8: Implement initiatives related to the security of certain documents used to enter the United States*<br>*DHS's comments:* According to DHS, our report's assessment of "generally not achieved" for this performance expectation reflects shifting criteria and does not take into account external factors beyond the department's control. DHS commented that an earlier draft of our report based a generally not achieved rating on a lack of evidence that DHS had addressed risks and challenges associated with the security of travel documents. DHS stated that our current report cites new issues relating to plans for the deployment of document readers and the development of a strategic plan for the Immigration Advisory Program. DHS also commented that the report does not take into consideration that Congress has delayed more extensive implementation of the Western Hemisphere Travel Initiative. DHS noted that despite these changes, it is on track and plans to implement the initiative at land and sea ports well in advance of the statutory deadline.<br>*Our response:* We considered all of DHS's additional information and documentation as part of our assessment. In doing so, we did not shift our criteria. Rather we disclosed our preliminary analysis and assessment to DHS in an earlier draft, received and analyzed additional documents, and updated our preliminary assessment based on the additional inputs. Our assessment recognized the extended timeframes for implementation of the Western Hemisphere Travel Initiative but also noted that this initiative has faced and continues to face implementation challenges despite the congressionally legislated extension of the implementation deadline. We noted that DHS has a long way to go to implement proposed plans for the initiative. |
| | *Performance expectation 12: Leverage technology, personnel, and information to secure the border*<br>*DHS's comments:* DHS commented that many of its programs currently leverage technology, personnel, and information to secure the border including US-VISIT, efforts to capture data on individuals attempting illegal entry into the United States between the ports of entry, as well as individuals who are being investigated or removed from the interior of the country. DHS reported that it takes advantage of the synergy from the efforts of both CBP and US-VISIT and leverages existing resources.<br>*Our response:* In our assessment, we recognize that although DHS has taken some actions to leverage technology, personnel, and information, much more work remains. For example, we reported that it is still unclear, and DHS has still not provided an adequate explanation of how US-VISIT will work with other border security initiatives. We also reported that while the Secure Border Strategic Plan provides some information on how various border security initiatives relate, the plan does not fully describe how these initiatives will interact once implemented. In addition, we noted that further development and implementation of SBI*net* would be key to achieving this performance expectation. |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| **Immigration enforcement** | *Performance expectation 2: Implement a program to ensure the timely identification and removal of aliens subject to removal from the United States*<br>*DHS's comments:* DHS commented that the methodology we used to reach this assessment is flawed because it dismisses tangible results in favor of potential challenges and holds DHS accountable for factors outside its control. DHS reported making progress in ensuring the timely identification of aliens subject to removal through programs to end the practice of "catch and release," increasing its detention bed space, shortening processing and detention times, and adding resources for interviewing consular officials about removal actions and for transporting aliens more quickly. DHS stated that certain variables impede the agency's ability to remove an alien including where expedited removal is halted or slowed due to certain foreign countries' unwillingness to accept their returned nationals and delays due to the lengthy duration of removal proceedings.<br>*Our response:* In our assessment, we recognize the difficulties DHS has faced in achieving this performance expectation due in part to factors beyond its control and highlight actions taken by DHS to address these challenges. Nevertheless, we believe that the assessment is appropriate and takes into account the challenges faced by DHS. For example, we reported that while DHS has taken actions to address challenges associated with foreign countries' unwillingness to provide travel documents for removing aliens, these efforts may not yet fully address the potential national security and public safety risks associated with DHS's inability to remove illegal aliens. We also reported that DHS has faced challenges in identifying aliens for removal and, according to the DHS IG, the fugitive alien population appears to be growing at a rate that exceeds Fugitive Operations Teams' ability to apprehend. Overall, DHS has implemented some efforts to achieve this performance expectation, but we believe that DHS can not yet ensure the timely identification and removal of aliens. |
| | *Performance expectation 3: Ensure the removal of criminal aliens*<br>*DHS's comments:* DHS expressed concern that our assessment for this performance expectation undervalues DHS's progress made through the Criminal Alien Program. DHS also commented that our report does not consider that the program is an ongoing, multiyear effort. DHS outlined its actions to ensure the removal of criminal aliens, including noting that 40 ICE operation teams presently screen foreign-born inmates and that ICE is continuing to train and hire nearly 200 additional staff to support the program and extend coverage to state and local jails and prisons. DHS indicated that fully implementing the Criminal Alien Program in all of the more than 5,000 federal, state, and local facilities across the country is an unrealistic expectation revealing a marked lack of appreciation for the enormous resources that would be required to implement such an expansion. According to DHS, even if it were appropriated the funds necessary to expand the program to a single additional institution every single day, it would take over eight years to achieve this outcome.<br>*Our response:* In our response, we acknowledge the difficult undertaking ICE is charged with in removing criminal aliens and have noted the various efforts underway, including DHS's efforts to expand the Criminal Alien Program. Our assessment is not intended to suggest that DHS should expand the Criminal Alien Program to every federal, state, and local correctional institution and jail. Rather, we reported that ICE has not expanded the program or taken other actions—such as reaching agreements with local law enforcement agencies—to ensure coverage for federal, state, and local correctional institutions and jails. Thus, ICE may not be able to fully ensure the removal of criminal aliens from facilities not covered by the Criminal Alien Program or agreements, and we concluded that DHS has generally not achieved this performance expectation. |

| Mission/<br>management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 6: Implement a program to allow for the secure alternative detention of noncriminal aliens*<br>*DHS's comments:* Although we did not make an assessment for this performance expectation, DHS commented that the information it provided to us demonstrated that programs for secure alternatives to detention of noncriminal aliens have been implemented. DHS highlighted its progress in implementing such programs and noted that our report drastically understates the level of meaningful participation in the alternatives to detection programs and the promising results already shown.<br>*Our response:* We did not make an assessment for this performance expectation because neither we nor the DHS IG had completed prior work, and we were unable to assess DHS's progress in achieving this performance expectation based on the information DHS provided. DHS provided us with procedures for its alternatives to detention program and data on the number of aliens enrolled in its programs and the rate of aliens' appearances in court and compliance with removal orders. We could not clearly determine the extent to which DHS has implemented program procedures, which we believe would be key to assessing DHS's progress. On the basis of our methodology, we believe that "no assessment" is appropriate for this performance expectation. |
| | *Performance expectation 8: Implement a prioritized worksite enforcement strategy to ensure that only authorized workers are employed*<br>*DHS's comments:* DHS stated that we have largely not considered its achievements in the worksite enforcement area and that DHS's efforts have resulted in impressive outcomes, including the increased use of employment verification systems and significant increases in investigations and arrests. For example, DHS reported making more than 4,300 worksite enforcement arrests and apprehensions in fiscal year 2006, and completing nearly 6,000 compliance enforcement investigations resulting in administrative arrests of more than 1,700 overstay and status violators, a 75 percent increase over the number of administrative arrests in fiscal year 2005.<br>*Our response:* We fully considered all of the information and documentation provided by DHS related to this performance expectation. In our assessment, we recognize the progress DHS has made in implementing its worksite enforcement program and outline DHS's program outputs, such as number of investigations conduced and arrests made. However, DHS did not provide us with evidence that it has established outcome-based goals and measures for its worksite enforcement program and the extent to which it has achieved desired outcomes for the program. We have previously reported that without outcome-based goals and measures, it will be difficult for ICE to fully determine whether its efforts are achieving desired outcomes. In addition, we highlighted challenges associated with DHS's Employment Eligibility Verification program, one of the requirements of the ICE Mutual Agreement between Government and Employers program, that would have to be fully addressed to help ensure the efficient and effective implementation of its strategy. |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 10: Implement a comprehensive strategy to interdict and prevent trafficking and smuggling of aliens into the United States*<br>*DHS's comments:* DHS commented that our assessment of "generally not achieved" is not supported by the facts provided to us. According to DHS, its strategy for counteracting the trafficking and smuggling of aliens is just one part of the larger Secure Border Initiative and Securing America's Border at the Ports of Entry Strategic Plan. DHS also stated that it has made significant progress in meeting this performance expectation in coordination with other departmental components and federal agencies. DHS pointed to Border Enforcement and Security Task Forces to target cross-border criminal activity, including human trafficking, and the ICE Trafficking in Persons Strategy to target criminal organizations and individuals engaged in human trafficking worldwide. DHS also stated that there are mechanisms in place for ICE and CBP to share information related to the trafficking or smuggling of aliens.<br>*Our response:* We fully considered all of the information and documentation DHS provided to us for this performance expectation. In our assessment, we recognize DHS's progress in implementing a strategy to interdict and prevent human trafficking and smuggling. However, we reported that the effectiveness of such a strategy depends on having clearly defined roles and responsibilities and goals and measures for assessing the extent to which DHS's efforts are achieving desired outcomes. We reported that until DHS has developed a mechanism to better share information among the responsible agencies and the ability to evaluate the outcome of its efforts, DHS will not have a comprehensive strategy in place, and we concluded that DHS has not yet generally achieved this performance expectation. |
| **Immigration services** | *Performance expectation 1: Eliminate the benefit application backlog and reduce application completion times to 6 months*<br>*DHS's comments:* DHS expressed disagreement with our assessment of "generally not achieved." According to DHS, it is well on its way to eliminating the application backlog, which it reported as of September 2006 was less than 10,000 applications. DHS expressed concern that we penalized DHS for not including in its definition of backlog cases instances where information from the applicant or another agency is pending. DHS commented that our report does not appropriately recognize external factors beyond the department's control—including delays by other agencies and the limitation on available visas. DHS also commented that our assessment for this performance expectation is inconsistent with other assessments made in the report that explicitly limit the scope of performance expectations to "DHS's roles and responsibilities."<br>*Our response:* In our assessment, we noted that while DHS has made significant progress in reducing the number of applications pending adjudication, USCIS's method of calculating its backlog leaves the possibility of individual cases pending for longer than 6 months, and USCIS stated that some applications received in 2004 and 2005, or even earlier, may still be pending. We reported that while giving lower priority to applications for which a benefit would not be immediately available or were awaiting action outside of USCIS is a reasonable approach to backlog reduction, those applications—1 million as of September 2006—were awaiting adjudication. We reported that adjudicating these applications would let applicants know their eligibility for benefits and could help prevent future delays if large numbers of those benefits became available, as happened when a 2005 law eliminated the annual cap on asylum beneficiaries. As we believe that adjudication of these applications is possible, we have applied our methodology consistently for this performance expectation. In addition, DHS's current data systems cannot produce backlog information based on the date of the filing of a benefit application, which is necessary under the congressional definition of "backlog." USCIS has also not yet demonstrated that it has overcome long-standing technology problems which have contributed to the backlog in the first place. |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 3: Establish a timetable for reviewing the program rules, business processes, and procedures for immigration benefit applications*<br>*DHS's comments:* DHS commented that our assessment of "generally not achieved" is not supported by the facts or documents provided to us. DHS noted that it has grouped its existing transactions into four major types of transactions handled—citizenship, immigrant, humanitarian, nonimmigrant—and has developed a timetable to implement improved processes for each of these four types of transactions contained in the DHS-USCIS Transformation Program Office FY 2007 Expenditure Plan. DHS expressed concern that we had not considered this timetable in our assessment.<br>*Our response:* DHS provided us the FY2007 Transformation Expenditure Plan, which we fully considered as part of our assessment. The plan contained general timetables for reviewing each activity by fiscal year. The FY 2007 Expenditure Plan states that the timelines and actual costs incurred will depend on the specific acquisition strategy defined for each increment. Additionally, DHS reported that it will prepare a detailed timetable for reviewing program rules, business processes, and procedures for each benefit category once it awards the contract. Until it does so, we concluded that DHS has generally not achieved this expectation. |
| | *Performance expectation 5: Develop new programs to prevent future backlogs from developing*<br>*DHS's comments:* According to DHS, our report does not give proper credit to the department's significant transformation efforts to increase resources, improve customer service, and modernize business practices relating to benefits applications. DHS expressed concern that we did not consider the issuance of a rule to adjust the Immigration and Naturalization Benefit Application and Petition Schedule to adjust fees collected for benefit applications. DHS stated that this adjustment will provide a stable source of revenue to support a significant reduction in processing times.<br>*Our response:* In our assessment for this performance expectation, we recognize revisions made by DHS to the Immigration and Naturalization Benefit Application and Petition Schedule. We recognize that raising fees may provide the agency with additional revenue and support its efforts to reduce processing times. However, we believe that raising fees alone will not ensure the prevention of future backlogs. Moreover, USCIS has initiated various programs to help reduce processing times, but these programs are still in the pilot stages and, in some cases, DHS has not yet assessed their results to determine the extent to which they could be implemented on a national basis. |
| | *Performance expectation 12: Establish training programs to reduce fraud in the benefits process*<br>*DHS 's comments:* According to DHS, it has developed a uniform training course for all officers. DHS also stated that it has identified certain fraud schemes that are unique to specific application processes and/or prevalent in geographical areas. The department consequently has provided specialized training to certain officers who handle these particular types of matters or who are stationed in certain locations above and beyond the uniform training provided to all officers. Instead of recognizing the achievements of these programs, DHS commented that our report appears to base its assessment of "generally not achieved" on the "appropriate[ness]" of the training, which appears to be an inconsistency of methodology.<br>*Our response:* In our assessment, we recognize USCIS's training programs focused on detecting fraud in the benefits process. However, DHS did not provide us with evidence on the extent to which it has taken actions to ensure that its training courses have been distributed and implemented appropriately across all of its field offices. DHS also did not provide us with evidence that it has taken actions to ensure that all staff receive training appropriate to their roles and responsibilities in adjudicating certain types of applications. Therefore, our assessment was not based on our evaluation of the appropriateness of the training but, rather, that DHS did not provide us with evidence showing that its staff have received the training applicable to their roles and responsibilities, which we believe is a key part of establishing programs to reduce benefit fraud. |

| Mission/<br>management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 14: Implement a fraud assessment program to reduce benefit fraud*<br>*DHS's comments:* DHS commented that the benefit fraud assessments it has conducted to date have provided useful baseline data to assist in the development of a comprehensive strategy. DHS reported that its assessments have resulted in procedural and regulatory changes to minimize certain types of fraud. DHS commented that our report states that it has not developed and demonstrated the success of a strategy for conducting assessments, while an earlier draft indicated that DHS had not provided evidence of recently completed assessments.<br>*Our response:* In our assessment, we noted that DHS has completed fraud assessments for three benefits types and expects to issue final reports on four others later in fiscal year 2007. However, we noted that USCIS has not yet developed and implemented a comprehensive strategy for conducting fraud assessments, which we believe is a key part of this expectation for DHS to implement a fraud assessment program. With regard to DHS's comments on differences between our final report and an earlier draft, for all of the performance expectations, we disclosed our preliminary analysis and assessments to DHS, received and analyzed the additional documents and statements from DHS officials, and updated our preliminary assessments based on the additional inputs. |
| **Aviation security** | *Performance expectation 2: Establish standards and procedures for effective airport perimeter security*<br>*DHS's comments:* DHS commented that our assessment for this performance expectation does not recognize the significance of the steps the department has taken in conjunction with airports and airlines to enhance perimeter security, such as inspection of vehicles at access gates and assessments of new technologies. DHS also noted that it provided us with documentation outlining the department's full compliance with relevant requirements established by the Aviation and Transportation Security Act. TSA commented that per Aviation and Transportation Security Act requirements, it has developed the Aviation Inspection Plan, which is based on an analytical risk assessment process evaluated threats, vulnerabilities, and potential consequences, and is reviews and updated every year. Further, DHS commented that we did not give sufficient consideration to the department's action plan for addressing recommendations from our 2004 report on airport perimeter security. In addition, DHS commented that it is difficult to precisely measure the deterrent effect of its measures for airport perimeter security.<br>*Our response:* In making our assessment, we considered all documents provided by DHS on steps taken to enhance airport perimeter security, including updated summaries of departmental policies and procedures and plans to assess relevant technology. While DHS has taken actions to enhance perimeter security, the department did not provide evidence that these actions have resulted in effective airport perimeter security, and it did not provide sufficient information or documentation that it had addressed all of the relevant requirements contained in the Aviation and Transportation Security Act and recommendations from our 2004 report. For example, DHS did not provide documentation showing that TSA has met an Aviation and Transportation Security Act requirement to recommend to airport operators commercially available measures or procedures for preventing unauthorized access to secured airport areas. In keeping with this requirement, we recommended in our 2004 report that DHS compile the results of technology assessments—those conducted by TSA as well as independent assessments by airport operators—and communicate the integrated results of these assessments to airport operators. DHS did not provide us with evidence that it has fully addressed this recommendation. |

| Mission/<br>management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 3: Establish standards and procedures to effectively control access to airport secured areas*<br>*DHS's comments:* DHS commented that our assessment for this performance expectation does not recognize the significance of the steps the department has taken to effectively control access to airport secured areas, such as development of the Aviation Direct Access Screening Program—which provides for the random screening of employees attempting to access secure areas—and background checks of employees before they are granted identification media. DHS noted that while it is difficult to precisely measure the deterrent effect of these actions, the department has determined that a random, risk-based approach to controlling access to secured areas is more effective than creating stationary screening stations. DHS also commented that it provided us with documentation outlining the department's full compliance with relevant requirements established by the Aviation and Transportation Security Act. Further, DHS stated that we did not give sufficient consideration to their action plan for addressing recommendations from our 2004 report.<br>O*ur response:* In making our assessment, we considered all documents provided by DHS on steps taken to strengthen access controls of secured areas, including updated information on its efforts to enhance security procedures for gate screening and security measures for issuing personnel identification media. While DHS has taken actions to enhance procedures for controlling access to airport secured areas, it did not provide us with evidence that these actions have resulted in effective access control for airport secured areas, and the DHS IG has identified continuing weaknesses in DHS's procedures to prevent unauthorized workers from accessing secured airport areas. Additionally, DHS did not provide sufficient information or documentation that it had addressed all of the relevant requirements contained in the Aviation and Transportation Security Act and recommendations from our 2004 report. For example, DHS did not provide documentation that TSA has met an Aviation and Transportation Security Act requirement to require vendors who have direct access to aircraft and to the airfield to develop security programs. We also did not receive documentation from DHS showing that the department had complied with our 2004 report recommendation to provide guidance and prioritized funding to airports for enhancing the security of the commercial airport system as a whole. |
| | *Performance expectation 14: Develop and implement an advanced prescreening system to allow DHS to compare domestic passenger information to the Selectee List and No Fly List*<br>*DHS's comments:* DHS commented that our assessment for this performance expectation does not recognize the department's progress in achieving milestones in its multiyear effort. DHS also believes that we did not consider all of the evidence the department provided detailing the Secure Flight program's mission needs, concept of operations, management plans, system requirements, acquisition plans, testing/evaluation plans, privacy assessments, and the related schedules.<br>*Our response:* In making our assessment, we considered the documents provided by DHS on Secure Flight's various plans, assessments and requirements, and concept of operations. As we have previously reported, DHS has on numerous occasions missed key development and implementation milestones it had established for the Secure Flight program. Due in part to DHS not following a disciplined development process for Secure Flight in 2006, DHS halted development of the program to begin a "rebaselining" which involves TSA reassessing program goals, requirements, and capabilities. DHS has since made some program changes and is continuing its efforts to develop Secure Flight. However, DHS has not yet completed development efforts for the program and has not yet implemented it. In addition, as this report provides an assessment of progress made by DHS during its first 4 years, we believe that it is appropriate to assess DHS's progress in achieving this performance expectation. |

| Mission/<br>management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 15: Develop and implement an international passenger prescreening process to compare passenger information to terrorist watch lists before aircraft departure*<br>*DHS's comments:* DHS commented that our assessment for this performance expectation prematurely assesses the department's progress on a long-term goal. The department noted that the Secure Flight Notice of Proposed Rule Making and the Pre-Departure Advanced Passenger Information System Final Rule are scheduled to be published in the coming months. According to DHS, these rulemakings will place the department on track to implement pre-departure international passenger screening. DHS commented that it does not appear that we considered these proposed rulemakings in making our assessment.<br>*Our response:* We considered the DHS proposed rulemaking for Advanced Passenger Information System as part of our assessment for this performance expectation. We did not consider the Secure Flight Notice of Proposed Rule Making because DHS stated that it would be published in the coming months. However, we have identified problems with implementation of the international prescreening process and have found that full implementation of an integrated domestic and international prescreening process is still several years away. In addition, as this report provides an assessment of progress made by DHS during its first 4 years, we believe that it is appropriate to assess DHS's progress in achieving this performance expectation. |
| | *Performance expectation 18: Deploy checkpoint technologies to address vulnerabilities*<br>*DHS's comments:* DHS commented that our assessment for this performance expectation does not recognize the department's progress and does not consider the practical limitations inherent in developing and deploying new technologies. According to DHS, it is constantly deploying existing and developing new technologies to reduce checkpoint vulnerabilities. In addition, DHS noted that we did not consider other efforts in addition to checkpoint technologies that have effectively reduced vulnerabilities, such as updated procedures to detect explosives, enhanced training for transportation security officers, specially-trained canine teams, and deployment of transportation security officers specifically trained in behavior recognition and bomb appraisal.<br>*Our response:* We recognize in our assessment of performance expectation 17 that DHS has generally achieved the expectation to develop and test checkpoint technologies to address vulnerabilities. DHS has made some enhancements to currently deployed technologies such as to metal detectors and x-ray machines. DHS is also pilot testing new technologies. However, DHS has had limited initial deployments of technology to provide additional levels of explosives security at checkpoints. Further, DHS reported in 2007 that extensive deployment of new technologies will not be realized for another 2 years. In addition, in our assessments for other performance expectations, we recognized DHS's efforts, other than technologies, to reduce vulnerabilities. For example, we considered DHS's updated procedures to detect explosives and the implementation of a training for transportation security officers in behavioral recognition and bomb appraisal in our assessment for performance expectation 16—develop and implement processes and procedures for physically screening passengers at airport checkpoints—and concluded that DHS generally achieved that expectation. |
| **Surface transportation security** | *Performance expectation 3: issue standards for securing surface transportation modes*<br>*DHS's comments:* DHS commented that while our assessment for this performance expectation recognized the department's issuance of standards related to mass transit and passenger and freight rail, it did not consider standards issued by the department in other transportation modes, including highways and pipelines. DHS noted that it developed and provided us with draft Security Action Items that contain standards, addressing personnel security, access control, and en route security for highway modality. DHS also outlined voluntary "smart practices" it has issued for pipeline security.<br>*Our response:* DHS has developed draft Security Action Items that contain standards related to highways, but has not yet finalized these standards. In general, the standards that have been issued are voluntary, and DHS has not identified whether these will be made mandatory. Moreover, the department did not provide us with documentation that it had developed standards for pipeline security. In accordance with our methodology and in absence of documentation verifying these standards, we concluded that DHS has generally not achieved this performance expectation. |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 4: Conduct compliance inspections for surface transportation systems*<br>*DHS's comments:* DHS believes that while our assessment recognizes that the department has conducted compliance inspections for mass transit, passenger rail, and freight rail, we did not give DHS credit for these compliance inspections or progress made in other areas. DHS outlined its efforts to conduct inspections for freight rail and mass transit systems and noted that Baseline Assessment and Security Enhancements reviews have been completed on 38 transportation systems.<br>*Our response:* In our assessment, we recognize DHS's efforts to conduct compliance inspections for surface transportation systems, including its Baseline Assessment and Security Enhancements reviews. Although DHS has deployed inspectors to conduct compliance inspections and carry out other security activities for mass transit, including passenger rail, and freight rail modes, DHS did not provide us with evidence that it has conducted compliance inspections for other surface transportation modes or information on whether the department believes compliance inspections are needed for other modes. In addition, we have reported that DHS's role of inspectors in enforcing security requirements has not been fully defined, and DHS did not provide us with documentation on its efforts to better define these roles. |
| **Maritime security** | *Performance expectation 16: Develop a long-range vessel-tracking system to improve maritime domain awareness*<br>*DHS's comments*: DHS stated that the assessment of "generally not achieved" demonstrates the problem of rating multi-year programs on the basis of whether total implementation has already been achieved, and the department provided examples of the progress it has made in achieving this expectation. DHS stated that by the end of 2007 the Coast Guard will receive identification and tracking information for vessels in U.S. waters in the vicinity of 55 critical ports and 9 coastal areas. The department also said that it is working to establish a Long Range Identification and Tracking system that will provide for global information on all U.S. flagged vessels required to carry transponders and information on all U.S.-bound vessels regardless of flag state within 1000 miles. Further, DHS stated that there are other vessel-tracking programs that fulfill the requirement for a long-range vessel tracking system. The department said that these programs are sensitive and consequently could not provide additional details in its comments.<br>*Our response*: While we understand that the development of a long-range vessel-tracking system is in process, our report is intended to provide an assessment of DHS's progress after 4 years. DHS has made progress in developing a long-range vessel-tracking and has vessel-tracking capabilities in place. However, based on publicly available information, it has not yet completed the development of its Long Range Identification and Tracking system that can provide coverage up to nautical 2,000 miles and is consistent with international treaties, conventions, and agreements. We believe this is key to DHS achieving this performance expectation. DHS has reported that the Coast Guard has vessel-tracking capabilities, but noted that work is needed in the processing, display, and training in the use of this information. In addition, DHS has reported that it has worked and is continuing to work with the International Maritime Organization to develop a long-range vessel tracking system and that an international agreement to implement a global tracking system by the end of 2008 has been reached. |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| Emergency preparedness and response | *Performance expectation 4: Ensure the capacity and readiness of disaster response teams*<br>*DHS's comments:* DHS believes that we did not give sufficient consideration to its disaster response team capacity and readiness improvements and outlined its various teams' capabilities. In particular, DHS highlighted its teams' response times following recent storms. DHS also reported that it is developing standardized doctrine, policies, response metrics, and operating procedures to support its new rapidly deployable response teams.<br>*Our response:* We considered all of the information provided by DHS on the capacity and readiness of its disaster response teams. DHS did not provide us with evidence that it has yet developed readiness indicators for most of its disaster response teams, which indicates that DHS cannot yet ensure the capacity and readiness of those teams. More broadly, DHS did not provide us with documentation of its teams' readiness and capacity, such as documentation on the results of exercises, tests, or after-action reports on the small-scale disasters in which the teams have been used. On the basis of our methodology and as DHS did not provide us with evidence verifying its disaster teams' readiness and capacity, we concluded that DHS has generally not achieved this performance expectation. |
| | *Performance expectation 7: Establish a single, all-hazards national response plan*<br>*DHS's comments:* DHS believes that we did not properly recognize the current National Response Plan, issued in 2004, and its annexes and Catastrophic Incident Supplement. DHS noted that the National Response Plan is being used daily to respond to incidents and is a "living document that will be regularly reviewed and revised." DHS also commented that the existing National Response Plan will be implemented in response to incidents that occur before the issuance of a revised plan and that there will be a transition process used in conjunction with issuance of any revised plan. DHS noted that our view that the National Response Plan will negatively impact the ability to fully train, exercise, and develop new implementation plans is flawed.<br>*Our response:* In our assessment for this performance expectation, we recognize DHS's issuance of the National Response Plan and its Catastrophic Incident Supplement. However, the lack of clarity and understanding of key roles and responsibilities under the plan was a major cause of many of the problems experienced in the response to Hurricane Katrina, and the changes made to the plan in 2006 only partially addressed these issues. Until the final revised plan is issued, federal, state, and local agencies cannot complete and test through exercises their operational plans for implementing any revised roles and responsibilities under the plan. For example, the Red Cross has said that its revised role in mass care and shelter will not take place until the National Response Plan review process is complete and all changes are approved. Moreover, the Secretary's recent designation of Principal Federal Officials and Federal Coordinating Officers raised new questions in Congress and among state and local officials regarding the roles and responsibilities of these officials and to whom they report and are responsible. In early August 2007 DHS circulated a revised version of the National Response Plan, now called the National Response Framework, but the Framework has not yet been formally circulated to state and local stakeholders for review and comment. Thus, it is still uncertain when the revision will be finalized. |
| | *Performance expectation 8: Coordinate implementation of a single all-hazards response plan*<br>*DHS's comments:* DHS believes that we have not given the department credit for the progress it has made in coordinating implementation of the existing National Response Plan. DHS commented that there has been extensive training, exercises, and planning efforts with federal, state, and local partners on implementation of the plan. DHS also noted that the coordinated responses to 97 major disaster declarations since Hurricane Katrina have allowed for greater coordination in the implementation of the National Response Plan.<br>*Our response:* Although DHS has said that it has coordinated responses to 97 major disaster declarations since Hurricane Katrina, none of these have been disasters of the scope of a major hurricane or catastrophic disaster. DHS did not provide us documentation on how coordination has been improved and assessed, how its training programs have contributed to more effective coordination, and how its improved coordination efforts can be applied to large-scale disasters. Absent this documentation and given concerns regarding the status of the revised National Response Plan, we concluded that DHS has generally not achieved this performance expectation. |

| Mission/<br>management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 13: Develop the capacity to provide needed emergency assistance and services in a timely manner*<br>*DHS's comments:* DHS commented that its critical services, such as improved logistics tracking and capacity; increased disaster victim registration; and robust fraud, waste, and abuse protection, are in place and fully functional. DHS noted that it has established and tested initiatives in logistics tracking and capacity, such as the Total Asset Visibility initiative, and has worked closely with state and local partners to identify and address their needs for disaster response. DHS also noted that it has engaged in disaster planning efforts to identify challenges that would result from major disasters in various areas of the nation. Overall, DHS commented that the majority of information it provided to us on this performance expectation was designed specifically to address catastrophic situations that are nearly impossible and very costly to simulate and that, in our assessment, we stated that it is difficult to assess DHS-FEMA's initiatives regarding this performance expectation.<br>*Our response:* In our assessment, we reported that DHS does not appear to have tested its various initiatives on a scale that reasonably simulates a major or catastrophic disaster and that, as a result, it is difficult to assess the results of DHS's various initiatives to improve its response to a major catastrophic disaster. However, as the basis for our assessment we noted that DHS did not provide us with documentation verifying that its emergency assistance capabilities are in place and capable of providing needed services in a timely manner following any incident. For example, DHS did not provide us with documentation on how it determined requirements for prepositioning disaster supplies to assess whether DHS has achieved its intended capacity, and DHS's optimization planning efforts for improvements to its logistics capabilities are still in the preliminary stages. According to our methodology, in the absence of documentation verifying DHS's actions, we concluded that DHS has generally not achieved this performance expectation. |
| | *Performance expectation 14: Provide timely assistance and services to individuals and communities in response to emergency events*<br>*DHS's comments:* DHS commented that it continues to develop and expand capabilities to provide timely assistance and services to individuals and communities in response to emergency events. For example, DHS reported undertaking initiatives and agreements to improve shelter management, support targeted registration assistance, and enable improved targeting of resources where needed. DHS reported that through its Public Assistance Program post-Katrina, DHS has obligated 80 percent of estimated assistance within an average of 150 days after declaration compared to 203 days prior to Katrina and exceeding DHS's goal of 180 days. DHS also noted that we did not recognize its achievements in updating policies, guidance, and training for debris removal and establishing a nationwide list of debris removal contractors. In addition, DHS commented that it has successfully responded to 107 major disasters, 15 emergencies, and 130 fires since Hurricane Katrina.<br>*Our response:* During our review, DHS did not provide us with documentation verifying the actions it has taken to provide timely assistance to individual and communities in response to emergency events. Moreover, DHS did not provide us with the results of tests or exercises of its emergency assistance and service capabilities. In the absence of such documentation verifying DHS's claims of actions taken to improve its capabilities, we concluded that DHS has generally not achieved this performance expectation. |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 15: Implement a program to improve interoperable communications among federal, state, and local agencies*<br>*DHS's comments:* DHS commented that our assessment does not fully credit the department for progress made by its Office of Emergency Communications and Office for Interoperability and Compatibility in improving federal agencies' interoperable communication capabilities. DHS outlined several initiatives aimed at developing programs related to interoperable communications, highlighting its Integrated Wireless Network to provide the Departments of Justice, Homeland Security, and Treasury with a consolidated federal wireless communications service. DHS noted that this network is aimed particularly at improving federal interoperability. DHS also noted that our report did not consider the practical realities associated with developing a communications system that will accommodate more than 50,000 emergency response agencies and where nearly 90 percent of the communications infrastructure is owned at the local level.<br>*Our response:* We considered all of the information and documentation provided by DHS on its efforts to implement a program to improve interoperable communications among federal, state, and local agencies. However, DHS is in the process of evaluating federal agencies' interoperable communications capabilities and did not provide us with documentation on its actions to improve interoperability between federal agencies and state and local agencies, which we believe is a key part of communications interoperability. In addition, as previously reported, the Integrated Wireless Network is mostly focused on improving interoperability among federal agencies, and the level of interoperability that state and local agencies will have with federal first responders on this network has not yet been decided. In our assessment, we reported that until a more concerted effort is made promote federal interoperability, overall progress in improving communications interoperability would remain limited. |
| | *Performance expectation 17: Increase the development and adoption of interoperability communications standards*<br>*DHS's comments:* DHS commented that our assessment for this performance expectation does not fully recognize the significant progress made by the department and appears to be based on shifting criteria used to evaluate DHS's progress. DHS outlined actions it has taken to increase the development and adoption of interoperability communications standards, including partnering with various entities to accelerate the Project 25 standards to develop and generate interoperable and compatible voice communications equipment irrespective of the manufacturer. DHS noted that our assessment is premature and inconsistent with the language of the performance expectation to increase the development and adoption of interoperability communications standards.<br>*Our response:* Our criteria for evaluating whether or not DHS has generally achieved this performance expectation did not change. DHS has taken actions to increase the development and adoption of interoperability communications standards, but more work needs to be done. In addition to completing undefined subsets of the standards, ambiguities in the defined subsets must be resolved in order to enable interoperability with radios built to these standards. |

| Mission/<br>management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 20: Provide guidance and technical assistance to first responders in developing and implementing interoperable communications capabilities*<br>*DHS's comments:* DHS commented that our assessment does not fully credit the department for progress made by its Office of Emergency Communications and Office for Interoperability and Compatibility. In its comments, DHS outlined several initiatives aimed at developing guidance and technical assistance related to interoperable communications, including the Interoperable Communications Technical Assistance Program. DHS noted that our assessment regarding SAFECOM's guidance and tools was based largely on limited feedback from four states and selected localities and that its experience suggests that numerous other entities have had success in using SAFECOM's guidance and tools.<br>*Our response:* As the basis for our assessment, we noted that (1) several states and localities were not aware of SAFECOM tools and guidance or did not find them useful and (2) DHS is in the process of developing measures to assess the extent of the use of its tools and guidance, but has not yet developed those measures. In addition, DHS did not provide us with documentation on states' and localities' use of guidance and tools or on the extent to which states and localities have found the guidance and tools useful. In accordance with our methodology and in the absence of such documentation, we concluded that DHS has generally not achieved this performance expectation. |
| | *Performance expectation 21: Provide assistance to state and local governments to develop all-hazards plans and capabilities*<br>*DHS's comments:* DHS commented that it has provided meaningful assistance to state and local governments to develop all-hazards plans and capabilities and outlines examples of this assistance in its comments. For example, DHS commented that our assessment largely relies on outdated GAO and DHS IG reports and does not reflect the department's recent efforts to include language in grant guidance to supports state and local governments' development of all-hazards plans and capabilities. DHS also commented that we reported that the department has been focused on funding terrorism preparedness rather than natural or all-hazards preparedness. DHS noted that while its National Planning Scenarios have focused in large part on terrorist events, this predominance is due to the fact that their unique and exacting capability requirements make them critical planning tools in the national effort to develop a truly all-hazards preparedness model. DHS also noted that in 2007 it has focused on multi-hazard mitigation with state and local governments and is engaged in efforts that develop state and local all-hazards capabilities.<br>*Our response:* DHS did not provide us with documentation on the extent to which its assistance to state and local governments has focused on all-hazards, nor on the extent to which it has helped state and local governments develop all-hazards capabilities. In accordance with our methodology and in the absence of such documentation verifying DHS's actions, we concluded that DHS has generally not achieved this performance expectation. |
| | *Performance expectation 24: Develop a system for collecting and disseminating lessons learned and best practices to emergency responders*<br>*DHS's comments:* DHS commented that our assessment does not reflect the substantial progress the department has made in developing the Lessons Learned Information Sharing Web site nor does it consider the practical difficulties associated with developing an online system. DHS reported making continuous improvements to the system, based on user feedback, and noted that additional improvements under development will address most, if not all, of the issues we previously raised about the system.<br>*Our response:* In our assessment, we recognize that DHS has developed and implemented the Lessons Learned Information Sharing System. In prior work, we identified various issues with the system. DHS has reported taking actions to address these issues, but these actions are not yet complete. In addition, it is unclear whether the system is actually collecting and disseminating lessons learned and best practices to emergency responders. |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| **Critical infrastructure and key resources protection** | *Performance expectation 3: Improve and enhance public/private information sharing involving attacks, threats, and vulnerabilities*<br>*DHS's comments*: DHS stated that it has made significant progress in information sharing. The department highlighted a number of efforts it has made in this area, such as the establishment of the Technical Resource for Incident Prevention system (TRIPwire) and the National Coordinating Center for Telecommunications. Further, DHS stated that we did not include an assessment of the private sector utilization of the Homeland Security Information Network. The department also stated that we relied largely on previous reports that do not account for its recent successes and noted that the DHS IG found that five recommendations from its report *Homeland Security Information Network Could Support Information Sharing More Effectively* (OIG-06-38) are considered resolved.<br>*Our response:* We reviewed DHS's updated information and considered the material it provided. While DHS demonstrated that it has created a number of information sharing programs, the department did not provide evidence demonstrating that these programs have actually improved information sharing. Specifically, DHS did not provide any metrics indicating that these programs have resulted in improved information sharing with federal, state, and local government or the private sector. In conducting our analysis we reviewed past and recent GAO and DHS IG reports concerning information sharing. Our April 2007 report, *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information–Sharing Initiatives* (GAO-07-455), found that DHS had not effectively coordinated the Homeland Security Information Network with key state and local initiatives and consequently faced the risk that information sharing is not occurring. We made four recommendations in this report. DHS concurred with three and indicated that it was taking actions to address each of them. In May 2007 we concluded that until DHS completes these efforts, such as developing an inventory of key state and local initiatives and fully implementing and institutionalizing key practices for effective coordination and collaboration, the department will continue to be at risk that information is not being effectively shared and that the department is duplicating state and local capabilities. Further, while the DHS IG stated in a July 11, 2007 letter that it considered resolved the five recommendations in its report OIG-06-38, it also stated that the recommendations would remain open until it received supporting documentation from the department. DHS identified actions it has taken to address the DHS IG's recommendations, and the DHS IG stated that these actions would satisfy its recommendations. However, the DHS IG stated that it needed evidence verifying DHS's activities before it could consider its recommendations closed. |

| Mission/<br>management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 4: Develop and enhance national analysis and warning capabilities for critical infrastructure*<br>*DHS's comments*: DHS stated that we do not give the department credit for advances it has made in achieving this performance expectation, particularly with regard to cyber critical infrastructure. DHS commented that in the area of cyber infrastructure, we inaccurately suggested that the department has provided no evidence of enhanced national warning capabilities. DHS also noted that our assessment does not consider the progress made by its National Cyber Security Division to develop and enhance cyber analysis, watch and warning, and collaboration with the private sector. DHS described efforts the U.S. Computer Readiness Team has made to conduct analysis, issue warnings, and collaborate with the public and private sector. The department also stated that its National Communications System and fusion centers have contributed to its analysis and warning efforts.<br>*Our response*: *Our response*: In previous GAO work, we reviewed the U.S. Computer Emergency Readiness Team and other DHS cyber security efforts. We reported that DHS through the U.S. Computer Emergency Readiness Team had made progress in providing analysis and warning capabilities, but had not resolved longstanding challenges concerning strategic analysis and warning capabilities, including methodological and data issues. Further, in the updated information and the response, DHS discussed several initiatives related to its analysis and warning capabilities. For example, it discusses a draft concept of operations for the private sector to handle incidents; however, until it is finalized and implemented, it is unclear whether the U.S. Computer Emergency Readiness Team's analysis and warning capabilities have been enhanced. Further, in the updated information DHS provided, the department described the Critical Infrastructure Warning Network as an essential component of its warning capabilities, but the department did not provide any documentation demonstrating it has improved those capabilities. The department also stated that the National Communication System and DHS's State and Local Fusion Center Program had analytical capabilities, but did not provide documentation demonstrating that they have enhanced national analysis and warning capabilities. In the absence of documentation verifying the accomplishments of theses efforts, we concluded that DHS has generally not achieved this performance expectation. |
| **Science and technology** | *Performance expectation 1: Develop a plan for departmental research, development, testing, and evaluation activities*<br>*DHS's comments:* DHS commented that our assessment for this performance expectation understates the significance of the department's June 2007 Science and Technology Strategic Plan. DHS noted that the plan describes yearly milestones and deliverables/goals for every project within the Science and Technology Directorate. DHS also commented that our assessment does not give the department credit for the strategic plan's description on the Science and Technology Directorate's organizational framework and risk-based research portfolio management strategy.<br>*Our response:* Our assessment recognizes the DHS Science and Technology Directorate's various plans, including its June 2007 strategic plan. As noted in our assessment, this performance expectation is based on the requirement in the Homeland Security Act of 2002 for the department to develop a strategic plan for identifying priorities, goals, objectives, and policies for, and coordinating the federal government's civilian efforts to identify an develop countermeasures to chemical, biological, and other emerging terrorist threats. According to the department, the June 2007 strategic plan does not address this requirement; therefore we concluded that DHS has generally not achieved this performance expectation. |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 2: Assess emerging chemical, biological, radiological, and nuclear threats and homeland security vulnerabilities*<br>*DHS's comments:* DHS commented that our assessment for this performance expectation does not account for the fact that the department's efforts to assess emerging vulnerabilities will always be ongoing and are not designed to reach a final end-goal completion. DHS outlined its efforts to assess threats and vulnerabilities, such as its completion of the Bio-Terrorism Risk Assessment in 2006, and noted that these ongoing efforts reflect real and meaningful progress by the department.<br>*Our response:* In our assessment we recognize those assessments that the department has completed as well as those that are underway. Specifically, while DHS has completed assessments on biological and chemical threats, other assessments for the chemical, radiological, and nuclear sectors are underway, and we believe that DHS's assessment efforts overall appear to be in the early stages. In addition, we recognize that DHS will be assessing threats and vulnerabilities on a regular basis; however, as this report provides an assessment of progress made by DHS during its first 4 years, we believe that it is appropriate to reach a conclusion that DHS has not yet generally achieved this performance expectation. |
| | *Performance expectation 3: Coordinate research, development, and testing efforts to identify and develop countermeasures to address chemical, biological, radiological, nuclear, and other emerging terrorist threats*<br>*DHS's comments:* DHS commented that our assessment for this performance expectation does not account for the fact that the department's efforts to develop countermeasures will always be ongoing and are not designed to reach a final end-goal completion. DHS outlined its various efforts to coordinate the research and development of countermeasures, highlighting, for example, its collaboration with other agencies and roles and responsibilities as part of interagency committees.<br>*Our response:* In our assessment we discuss DHS's activities to coordinate the research and development of countermeasures. However, we have identified concerns regarding DHS's coordination efforts. For example, we reported that DHS has not always comprehensively collected and shared testing information on radiation portal monitors. In addition, we believe that until DHS more fully completes its assessments of threats and vulnerabilities, it may not fully know what technologies or countermeasures and associated requirements are needed to address identified threat and vulnerabilities. |
| **Human capital management** | *Performance expectation 8: Implement training and development programs in support of DHS's mission and goals*<br>*DHS's comments:* DHS stated that the assessment of "generally not achieved" highlights the problems in using a binary standard to assess a multi-year program. The department stated that the Human Capital Operational Plan is a two year endeavor and that DHS has been meeting its targets within the plan. The department described several of its training and development efforts, such as DHScovery and the establishment of the National Capital Region Homeland Security Academy.<br>*Our response:* While we understand that the implementation of training and development programs is in process, our report is intended to provide an assessment of DHS's progress after 4 years. The Human Capital Operational Plan identifies 20 goals in its learning and development section, and DHS has met the 3 goals with deadlines earlier than June 1, 2007. The Human Capital Operational Plan contains 4 goals with deadlines that fall between June 1, 2007 and the release of this report, but we do not have information as to whether they were achieved. However, as the Human Capital Operational Plan indicates, the majority of department's learning and development goals—the remaining 13—are yet to be implemented. Given this, we concluded that DHS had not yet achieved this performance expectation. |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| **Information technology management** | *Performance expectation 5: Develop a comprehensive enterprise architecture*<br>*DHS's comments:* DHS commented that we based our assessment on a belief that DHS had not fully implemented elements of our Enterprise Architecture Management Maturity Framework and that we disregarded its extensive consultation with stakeholders in developing its architecture. The department further commented that our original assessment of "generally not achieved" was not consistent with the Office of Management and Budget's rating of the latest version of the department's architecture, referred to as DHS EA 2007, as a 4.3 on a scale from 1 to 5 for completeness.<br>*Our response:* We disagree that our assessment does not consider the department's progress in satisfying the Enterprise Architecture Management Maturity Framework or its consultation with stakeholders in developing its architecture. In particular, we recognized that DHS had fully implemented 24 of the 31 core elements of the Enterprise Architecture Management Maturity Framework, and that it solicited comments from its architecture stakeholders. However, we also recognized that key Enterprise Architecture Management Maturity Framework core elements had nevertheless not been completely implemented and that the latest version of the architecture that we had received and evaluated (i.e., DHS EA 2006) did not fully address stakeholder comments and recommendations that we had previously made aimed at adding missing architecture content. Moreover, we found that stakeholder commentary on this version was limited (e.g., major DHS organizations such as the Transportation Security Agency and Coast Guard did not even provide comments). Notwithstanding this, we also recognize that the department has since released a newer, more current version of its architecture (i.e., DHS EA 2007), which it provided to us in June 2007, and that the department reports that this version addresses many of our prior concerns and has been recently rated by the Office of Management and Budget as 4.3 on a scale of 1 to 5 for completeness. Because of the considerable time and resources necessary to evaluate an architecture as large and complex as DHS's, we have not had an opportunity to validate DHS's statements about this latest version. Moreover, we have not evaluated either the Office of Management and Budget's enterprise architecture assessment methodology or how it applied the methodology in assessing DHS EA 2007. As a result, we do not have a basis for concluding whether this more recent version of DHS's architecture does or does not generally achieve this performance expectation. Accordingly, we have modified our assessment of this performance expectation to "no assessment made". |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 6: Implement a comprehensive enterprise architecture*<br>*DHS's comments:* DHS commented that our assessment relied on an "allegation" that the department's information technology investments have not been fully aligned with its architecture. The department further commented that it had provided us with documentation of its methodology for assessing information technology investments relative to its enterprise architecture but that it appeared that we did not consider it. In addition, DHS commented that it has already implemented a comprehensive enterprise architecture as evidenced by the Office of Management and Budget's rating of DHS EA 2007 as a 4.5 on a scale from 1 to 5 for architecture use.<br>*Our response:* We disagree that our assessment relied on an allegation and did not consider documentation the department provided to us. First, our work was performed in accordance with professional auditing standards, and thus it in no way cites or relies on allegations. Rather, it is based on facts and evidence, or in this case the absence thereof. More specifically, our assessment is based on analyses that we conducted between 2003 and 2007 related to major information technology investments (e.g., US-VISIT) in which DHS did not provide sufficient documentation and verifiable analysis demonstrating these investments' alignment to any version of the DHS architecture. We further disagree that we did not consider documentation that the department provided us that it characterized in its comments as describing its methodology for assessing information technology investments relative to its enterprise architecture. In point of fact, we analyzed the documents the department provided and determined that they described a process that required information technology investment compliance with the enterprise architecture but did not include a methodology with detailed compliance criteria. In our view, the existence and application of such criteria is necessary to implementing an enterprise architecture. As we have previously reported and as is reflected in federal guidance and best practices, both a methodology and explicit criteria for determining an investment's alignment with an enterprise architecture are essential to understanding the risk associated with areas of noncompliance. Accordingly, we have open recommendations to the department for establishing and applying both, as well as for disclosing the risks on major investments of not having done so. With respect to the department's claim that the Office of Management and Budget's rating on its architecture's use is evidence that it has already implemented a comprehensive architecture, we have no basis for commenting on the rating. However, our view is that it is not possible to effectively implement any enterprise architecture without an architecture compliance methodology and criteria. Accordingly, we have not changed our assessment of this performance expectation. |
| | *Performance expectation 7: Develop a process to effectively manage information technology investments*<br>*DHS's comments:* DHS commented that our assessment does not accurately reflect the department's progress and that it has developed processes to effectively manage information technology investments. Specifically, DHS stated that it had developed and distributed the *Periodic Reporting*, *Earned Value Management*, and *Operational Analysis* guidance documents for improving the tracking and reporting of investment costs, schedules, and performance variances. DHS also noted that it had issued a management directive that provides the DHS Chief Information Officer with the authority to review and approve the Department's entire information technology budget.<br>*Our response:* We disagree that our assessment does not accurately reflect DHS's progress in developing processes to effectively manage information technology investments. In fact, our assessment is based, among other things, on the guidance documents that DHS cited and is reflected in our April 2007 report in which we concluded that DHS had established the management structure to effectively manage its investments but had yet to fully define 8 of the 11 related policies and procedures that are defined in the GAO Information Technology Investment Management Framework. For example, DHS's procedures for selecting investments did not cite either the specific criteria or steps for prioritizing and selecting new information technology proposals. In written comments on our April report, DHS agreed with our report. In addition, we agree that DHS issued a directive expanding the authority of the Chief Information Officer, as we recognized in assessing the Chief Information Officer's roles and responsibilities as generally achieved. However, this directive does not affect our findings and conclusions relative to the 8 policies and procedures in our framework that were not satisfied. As a result, our assessment remains as generally not achieved. |

| Mission/ management area | Summary of DHS's comments and our response |
|---|---|
| | *Performance expectation 8: Implement a process to effectively manage information technology investments*<br>*DHS's comments:* DHS commented that our assessment does not accurately reflect the department's progress. In particular, the department stated that it has implemented an information technology acquisition review process to improve the alignment of information technology purchases to the department's homeland security mission and architecture. In addition, DHS reported that its information technology portfolio management program incorporates specific management processes to improve the balance of investments to more effectively meet departmental goals and objectives.<br>*Our response:* We disagree that our assessment does not accurately reflect DHS' progress in implementing processes to effectively manage information technology investments. Our assessment is based on our April 2007 report in which we concluded that DHS had not fully implemented any of the key practices in the GAO Information Technology Investment Management Framework associated with actually controlling investments at either the project or the portfolio level. For example, we reported that the investment review boards had not conducted regular reviews of investments and that while control activities were sometimes performed, they were not performed consistently across information technology projects. In commenting on our report, DHS agreed with our findings and recommendations. As a result, our assessment remains as generally not achieved. |

Source: GAO analysis.

As arranged with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days after the date of this report. At that time, we will send copies of this report to the Secretary of Homeland Security, the Director of the Office of Management and Budget, and appropriate congressional committees. We will also make copies available to others upon request. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staff has any questions regarding this report, please contact me at (202) 512-8777, or rabkinn@gao.gov. Contact points for each mission and management area are listed in appendix I. Contact points for our Offices of Congressional Relations and Public Affairs may be found on this last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Norman Rabkin

Norman J. Rabkin
Managing Director, Homeland Security and Justice Issues

# Appendix I: Key GAO Contacts for DHS Mission and Management Areas

| | |
|---|---|
| Border Security | Richard Stana, Director, Homeland Security and Justice, 202-512-8816<br>Jess Ford, Director, International Affairs and Trade, 202-512-4128 |
| Immigration Enforcement and Immigration Services | Richard Stana, Director, Homeland Security and Justice, 202-512-8816 |
| Aviation Security | Cathleen Berrick, Director, Homeland Security and Justice, 202-512-3404 |
| Surface Transportation Security | Cathleen Berrick, Director, Homeland Security and Justice, 202-512-3404<br>Katherine Siggerud, Director, Physical Infrastructure, 202-512-2834 |
| Maritime Security | Stephen L. Caldwell, Director, Homeland Security and Justice, 202-512-9610 |
| Emergency Preparedness and Response | William O Jenkins, Jr., Director, Homeland Security and Justice, 202-512-8757<br>Linda Koontz, Director, Information Technology, 202-512-7487 |
| Critical Infrastructure and Key Resources Protection | Eileen R. Larence, Director, Homeland Security and Justice, 202-512-8777<br>David A. Powner, Director, Information Technology Management Issues, 202-512-9286<br>John R. Stephenson, Director, Natural Resources and Environment, 202-512-3841 |
| Science and Technology | Gene Aloise, Director, Natural Resources and Environment, 202-512-3841<br>Keith Rhodes, Chief Technologist, 202-512-6412 |

## Acquisition Management

John P. Hutton, Director, Acquisition Management and Sourcing, 202-512-4841

William T. Woods, Director, Acquisition Management and Sourcing, 202-512-4841

## Financial Management

McCoy Williams, Director, Financial Management and Assurance, 202-512-9095

## Human Capital Management

J. Christopher Mihm, Managing Director, Strategic Issues, 202-512-6806

## Information Technology Management

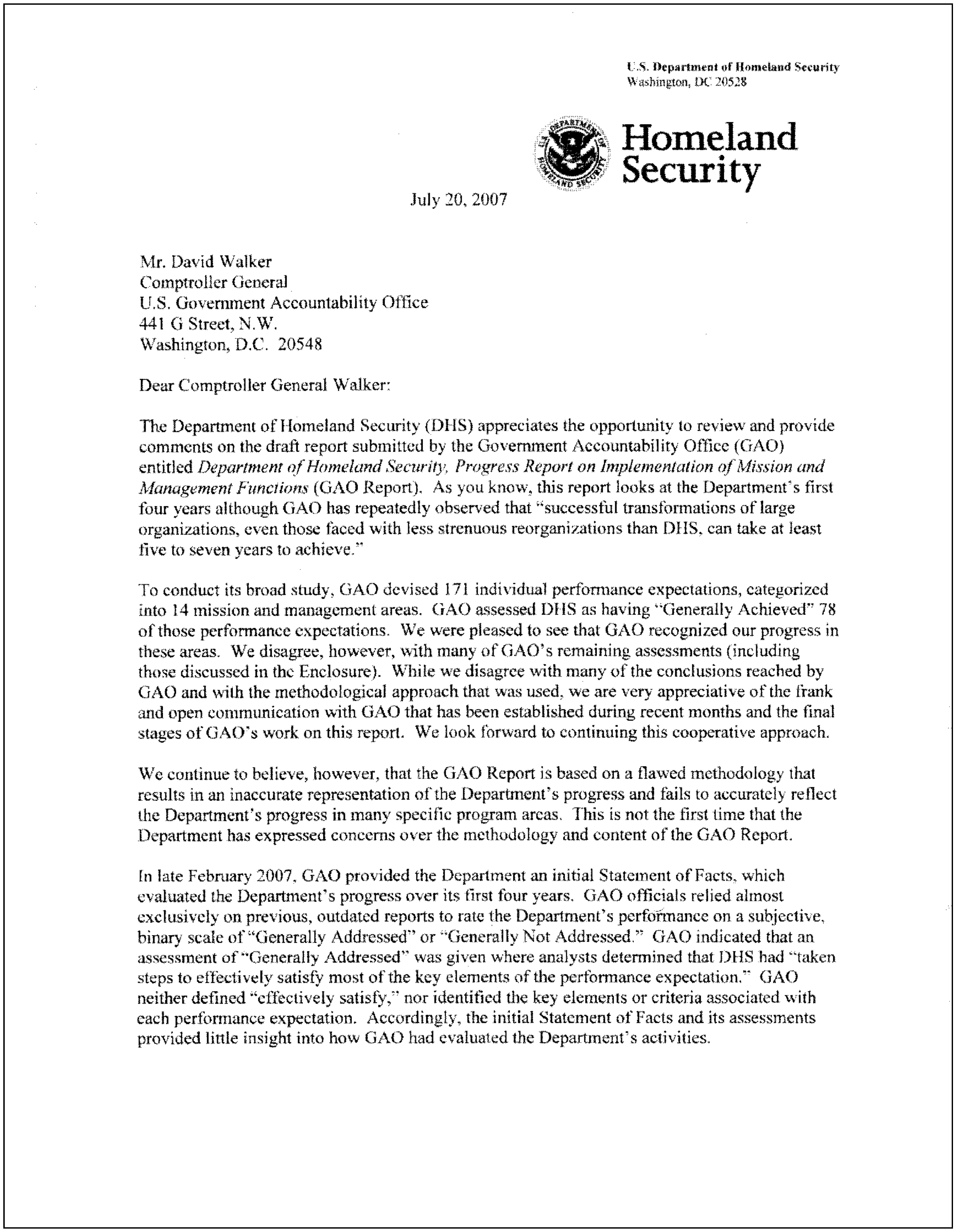
Randolph Hite, Director, Information Technology, 202-512-3439

Gregory Wilshusen, Director, Information Technology, 202-512-6244

## Real Property Management

Mark Goldstein, Director, Physical Infrastructure, 202-512-2834

# Appendix II: Comments from the Department of Homeland Security



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

Homeland
Security

July 20, 2007

Mr. David Walker
Comptroller General
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

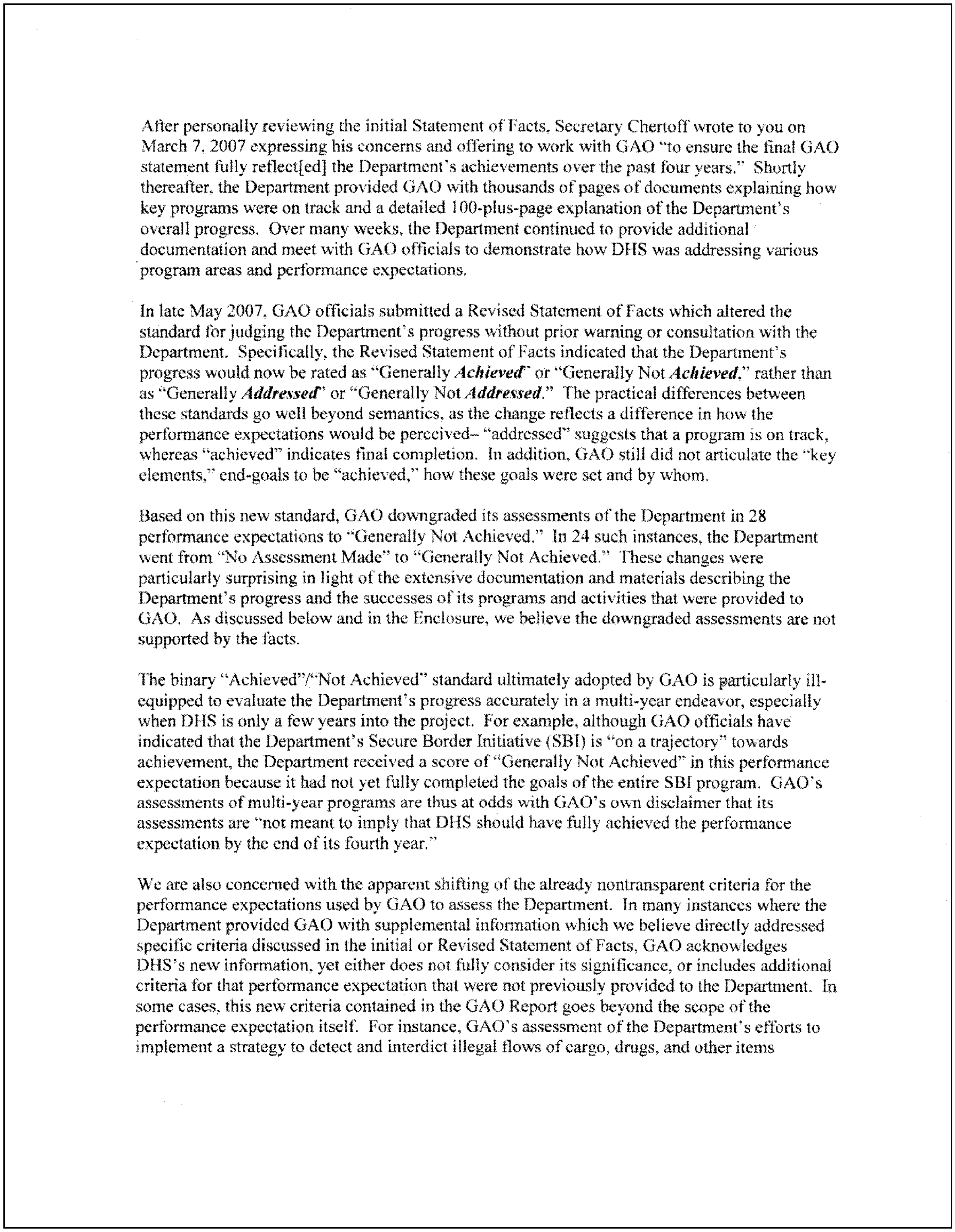
Dear Comptroller General Walker:

The Department of Homeland Security (DHS) appreciates the opportunity to review and provide comments on the draft report submitted by the Government Accountability Office (GAO) entitled *Department of Homeland Security, Progress Report on Implementation of Mission and Management Functions* (GAO Report). As you know, this report looks at the Department's first four years although GAO has repeatedly observed that "successful transformations of large organizations, even those faced with less strenuous reorganizations than DHS, can take at least five to seven years to achieve."

To conduct its broad study, GAO devised 171 individual performance expectations, categorized into 14 mission and management areas. GAO assessed DHS as having "Generally Achieved" 78 of those performance expectations. We were pleased to see that GAO recognized our progress in these areas. We disagree, however, with many of GAO's remaining assessments (including those discussed in the Enclosure). While we disagree with many of the conclusions reached by GAO and with the methodological approach that was used, we are very appreciative of the frank and open communication with GAO that has been established during recent months and the final stages of GAO's work on this report. We look forward to continuing this cooperative approach.

We continue to believe, however, that the GAO Report is based on a flawed methodology that results in an inaccurate representation of the Department's progress and fails to accurately reflect the Department's progress in many specific program areas. This is not the first time that the Department has expressed concerns over the methodology and content of the GAO Report.

In late February 2007, GAO provided the Department an initial Statement of Facts, which evaluated the Department's progress over its first four years. GAO officials relied almost exclusively on previous, outdated reports to rate the Department's performance on a subjective, binary scale of "Generally Addressed" or "Generally Not Addressed." GAO indicated that an assessment of "Generally Addressed" was given where analysts determined that DHS had "taken steps to effectively satisfy most of the key elements of the performance expectation." GAO neither defined "effectively satisfy," nor identified the key elements or criteria associated with each performance expectation. Accordingly, the initial Statement of Facts and its assessments provided little insight into how GAO had evaluated the Department's activities.



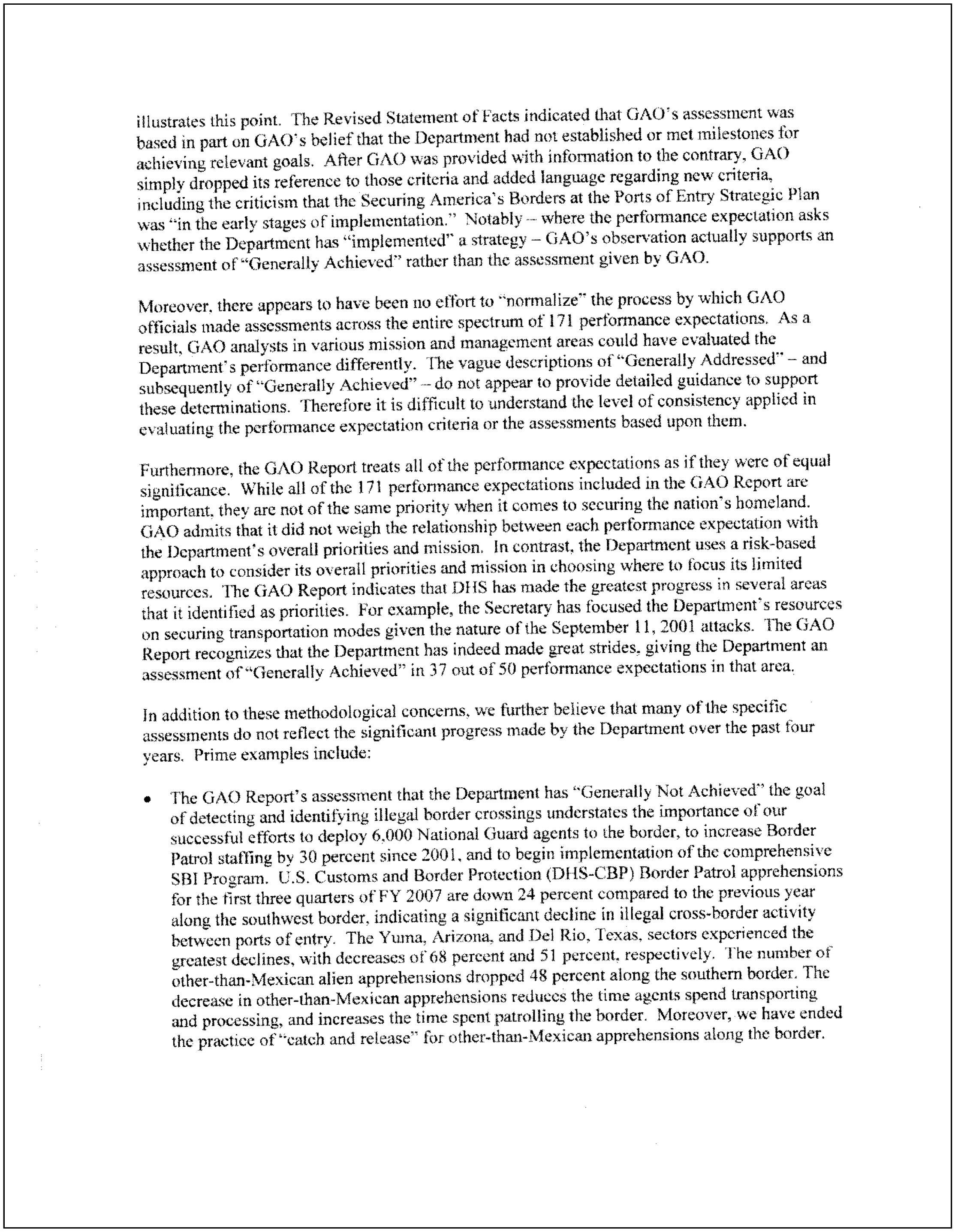
After personally reviewing the initial Statement of Facts, Secretary Chertoff wrote to you on March 7, 2007 expressing his concerns and offering to work with GAO "to ensure the final GAO statement fully reflect[ed] the Department's achievements over the past four years." Shortly thereafter, the Department provided GAO with thousands of pages of documents explaining how key programs were on track and a detailed 100-plus-page explanation of the Department's overall progress. Over many weeks, the Department continued to provide additional documentation and meet with GAO officials to demonstrate how DHS was addressing various program areas and performance expectations.

In late May 2007, GAO officials submitted a Revised Statement of Facts which altered the standard for judging the Department's progress without prior warning or consultation with the Department. Specifically, the Revised Statement of Facts indicated that the Department's progress would now be rated as "Generally ***Achieved***" or "Generally Not ***Achieved***," rather than as "Generally ***Addressed***" or "Generally Not ***Addressed***." The practical differences between these standards go well beyond semantics, as the change reflects a difference in how the performance expectations would be perceived– "addressed" suggests that a program is on track, whereas "achieved" indicates final completion. In addition, GAO still did not articulate the "key elements," end-goals to be "achieved," how these goals were set and by whom.

Based on this new standard, GAO downgraded its assessments of the Department in 28 performance expectations to "Generally Not Achieved." In 24 such instances, the Department went from "No Assessment Made" to "Generally Not Achieved." These changes were particularly surprising in light of the extensive documentation and materials describing the Department's progress and the successes of its programs and activities that were provided to GAO. As discussed below and in the Enclosure, we believe the downgraded assessments are not supported by the facts.

The binary "Achieved"/"Not Achieved" standard ultimately adopted by GAO is particularly ill-equipped to evaluate the Department's progress accurately in a multi-year endeavor, especially when DHS is only a few years into the project. For example, although GAO officials have indicated that the Department's Secure Border Initiative (SBI) is "on a trajectory" towards achievement, the Department received a score of "Generally Not Achieved" in this performance expectation because it had not yet fully completed the goals of the entire SBI program. GAO's assessments of multi-year programs are thus at odds with GAO's own disclaimer that its assessments are "not meant to imply that DHS should have fully achieved the performance expectation by the end of its fourth year."

We are also concerned with the apparent shifting of the already nontransparent criteria for the performance expectations used by GAO to assess the Department. In many instances where the Department provided GAO with supplemental information which we believe directly addressed specific criteria discussed in the initial or Revised Statement of Facts, GAO acknowledges DHS's new information, yet either does not fully consider its significance, or includes additional criteria for that performance expectation that were not previously provided to the Department. In some cases, this new criteria contained in the GAO Report goes beyond the scope of the performance expectation itself. For instance, GAO's assessment of the Department's efforts to implement a strategy to detect and interdict illegal flows of cargo, drugs, and other items



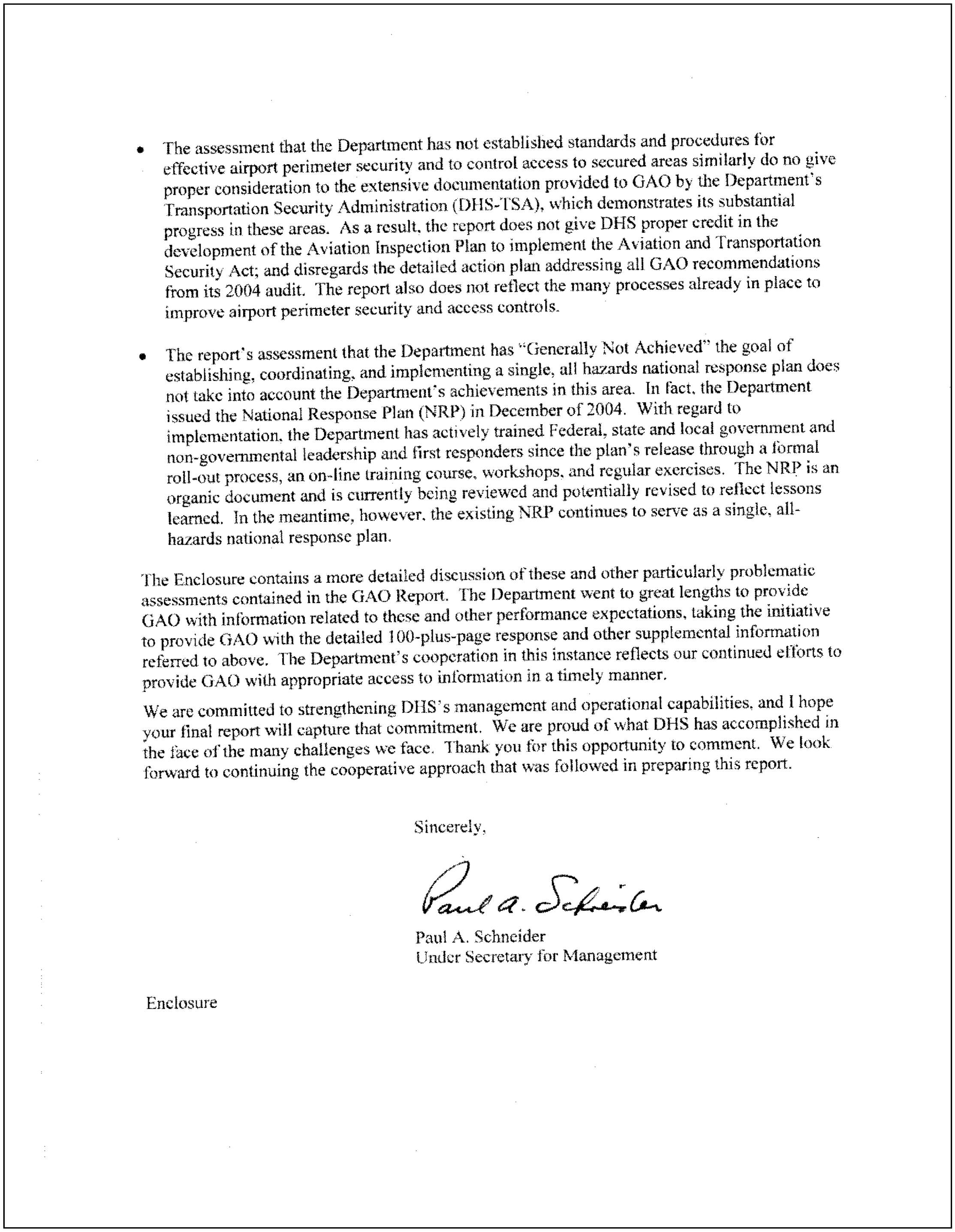
illustrates this point. The Revised Statement of Facts indicated that GAO's assessment was based in part on GAO's belief that the Department had not established or met milestones for achieving relevant goals. After GAO was provided with information to the contrary, GAO simply dropped its reference to those criteria and added language regarding new criteria, including the criticism that the Securing America's Borders at the Ports of Entry Strategic Plan was "in the early stages of implementation." Notably – where the performance expectation asks whether the Department has "implemented" a strategy – GAO's observation actually supports an assessment of "Generally Achieved" rather than the assessment given by GAO.

Moreover, there appears to have been no effort to "normalize" the process by which GAO officials made assessments across the entire spectrum of 171 performance expectations. As a result, GAO analysts in various mission and management areas could have evaluated the Department's performance differently. The vague descriptions of "Generally Addressed" – and subsequently of "Generally Achieved" – do not appear to provide detailed guidance to support these determinations. Therefore it is difficult to understand the level of consistency applied in evaluating the performance expectation criteria or the assessments based upon them.

Furthermore, the GAO Report treats all of the performance expectations as if they were of equal significance. While all of the 171 performance expectations included in the GAO Report are important, they are not of the same priority when it comes to securing the nation's homeland. GAO admits that it did not weigh the relationship between each performance expectation with the Department's overall priorities and mission. In contrast, the Department uses a risk-based approach to consider its overall priorities and mission in choosing where to focus its limited resources. The GAO Report indicates that DHS has made the greatest progress in several areas that it identified as priorities. For example, the Secretary has focused the Department's resources on securing transportation modes given the nature of the September 11, 2001 attacks. The GAO Report recognizes that the Department has indeed made great strides, giving the Department an assessment of "Generally Achieved" in 37 out of 50 performance expectations in that area.

In addition to these methodological concerns, we further believe that many of the specific assessments do not reflect the significant progress made by the Department over the past four years. Prime examples include:

- The GAO Report's assessment that the Department has "Generally Not Achieved" the goal of detecting and identifying illegal border crossings understates the importance of our successful efforts to deploy 6,000 National Guard agents to the border, to increase Border Patrol staffing by 30 percent since 2001, and to begin implementation of the comprehensive SBI Program. U.S. Customs and Border Protection (DHS-CBP) Border Patrol apprehensions for the first three quarters of FY 2007 are down 24 percent compared to the previous year along the southwest border, indicating a significant decline in illegal cross-border activity between ports of entry. The Yuma, Arizona, and Del Rio, Texas, sectors experienced the greatest declines, with decreases of 68 percent and 51 percent, respectively. The number of other-than-Mexican alien apprehensions dropped 48 percent along the southern border. The decrease in other-than-Mexican apprehensions reduces the time agents spend transporting and processing, and increases the time spent patrolling the border. Moreover, we have ended the practice of "catch and release" for other-than-Mexican apprehensions along the border.



- The assessment that the Department has not established standards and procedures for effective airport perimeter security and to control access to secured areas similarly do no give proper consideration to the extensive documentation provided to GAO by the Department's Transportation Security Administration (DHS-TSA), which demonstrates its substantial progress in these areas. As a result, the report does not give DHS proper credit in the development of the Aviation Inspection Plan to implement the Aviation and Transportation Security Act; and disregards the detailed action plan addressing all GAO recommendations from its 2004 audit. The report also does not reflect the many processes already in place to improve airport perimeter security and access controls.

- The report's assessment that the Department has "Generally Not Achieved" the goal of establishing, coordinating, and implementing a single, all hazards national response plan does not take into account the Department's achievements in this area. In fact, the Department issued the National Response Plan (NRP) in December of 2004. With regard to implementation, the Department has actively trained Federal, state and local government and non-governmental leadership and first responders since the plan's release through a formal roll-out process, an on-line training course, workshops, and regular exercises. The NRP is an organic document and is currently being reviewed and potentially revised to reflect lessons learned. In the meantime, however, the existing NRP continues to serve as a single, all-hazards national response plan.

The Enclosure contains a more detailed discussion of these and other particularly problematic assessments contained in the GAO Report. The Department went to great lengths to provide GAO with information related to these and other performance expectations, taking the initiative to provide GAO with the detailed 100-plus-page response and other supplemental information referred to above. The Department's cooperation in this instance reflects our continued efforts to provide GAO with appropriate access to information in a timely manner.

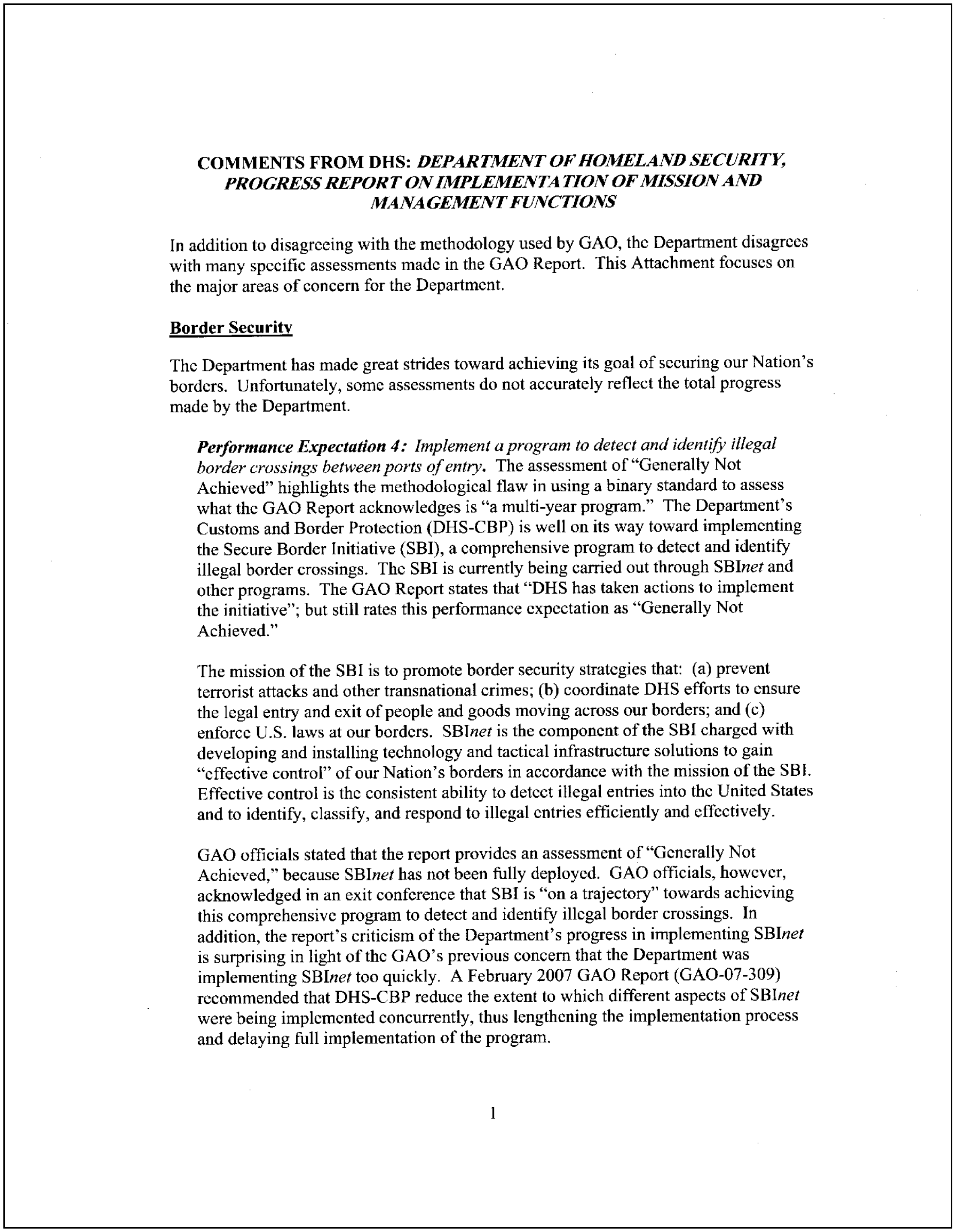
We are committed to strengthening DHS's management and operational capabilities, and I hope your final report will capture that commitment. We are proud of what DHS has accomplished in the face of the many challenges we face. Thank you for this opportunity to comment. We look forward to continuing the cooperative approach that was followed in preparing this report.

Sincerely,

Paul a. Schneider

Paul A. Schneider
Under Secretary for Management

Enclosure



## COMMENTS FROM DHS: *DEPARTMENT OF HOMELAND SECURITY, PROGRESS REPORT ON IMPLEMENTATION OF MISSION AND MANAGEMENT FUNCTIONS*

In addition to disagreeing with the methodology used by GAO, the Department disagrees with many specific assessments made in the GAO Report. This Attachment focuses on the major areas of concern for the Department.

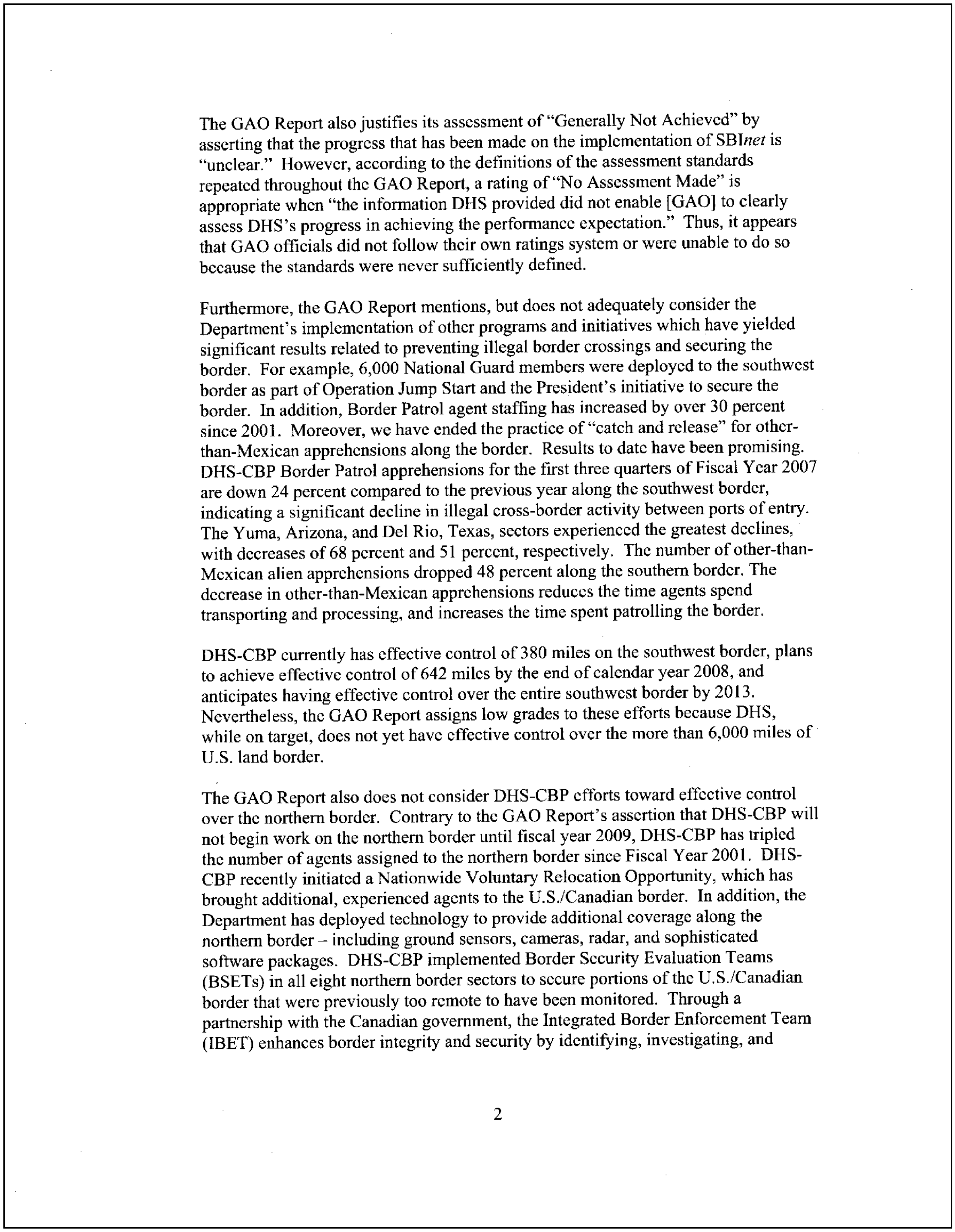
### Border Security

The Department has made great strides toward achieving its goal of securing our Nation's borders. Unfortunately, some assessments do not accurately reflect the total progress made by the Department.

***Performance Expectation 4:*** *Implement a program to detect and identify illegal border crossings between ports of entry.* The assessment of "Generally Not Achieved" highlights the methodological flaw in using a binary standard to assess what the GAO Report acknowledges is "a multi-year program." The Department's Customs and Border Protection (DHS-CBP) is well on its way toward implementing the Secure Border Initiative (SBI), a comprehensive program to detect and identify illegal border crossings. The SBI is currently being carried out through SBI*net* and other programs. The GAO Report states that "DHS has taken actions to implement the initiative"; but still rates this performance expectation as "Generally Not Achieved."

The mission of the SBI is to promote border security strategies that: (a) prevent terrorist attacks and other transnational crimes; (b) coordinate DHS efforts to ensure the legal entry and exit of people and goods moving across our borders; and (c) enforce U.S. laws at our borders. SBI*net* is the component of the SBI charged with developing and installing technology and tactical infrastructure solutions to gain "effective control" of our Nation's borders in accordance with the mission of the SBI. Effective control is the consistent ability to detect illegal entries into the United States and to identify, classify, and respond to illegal entries efficiently and effectively.

GAO officials stated that the report provides an assessment of "Generally Not Achieved," because SBI*net* has not been fully deployed. GAO officials, however, acknowledged in an exit conference that SBI is "on a trajectory" towards achieving this comprehensive program to detect and identify illegal border crossings. In addition, the report's criticism of the Department's progress in implementing SBI*net* is surprising in light of the GAO's previous concern that the Department was implementing SBI*net* too quickly. A February 2007 GAO Report (GAO-07-309) recommended that DHS-CBP reduce the extent to which different aspects of SBI*net* were being implemented concurrently, thus lengthening the implementation process and delaying full implementation of the program.

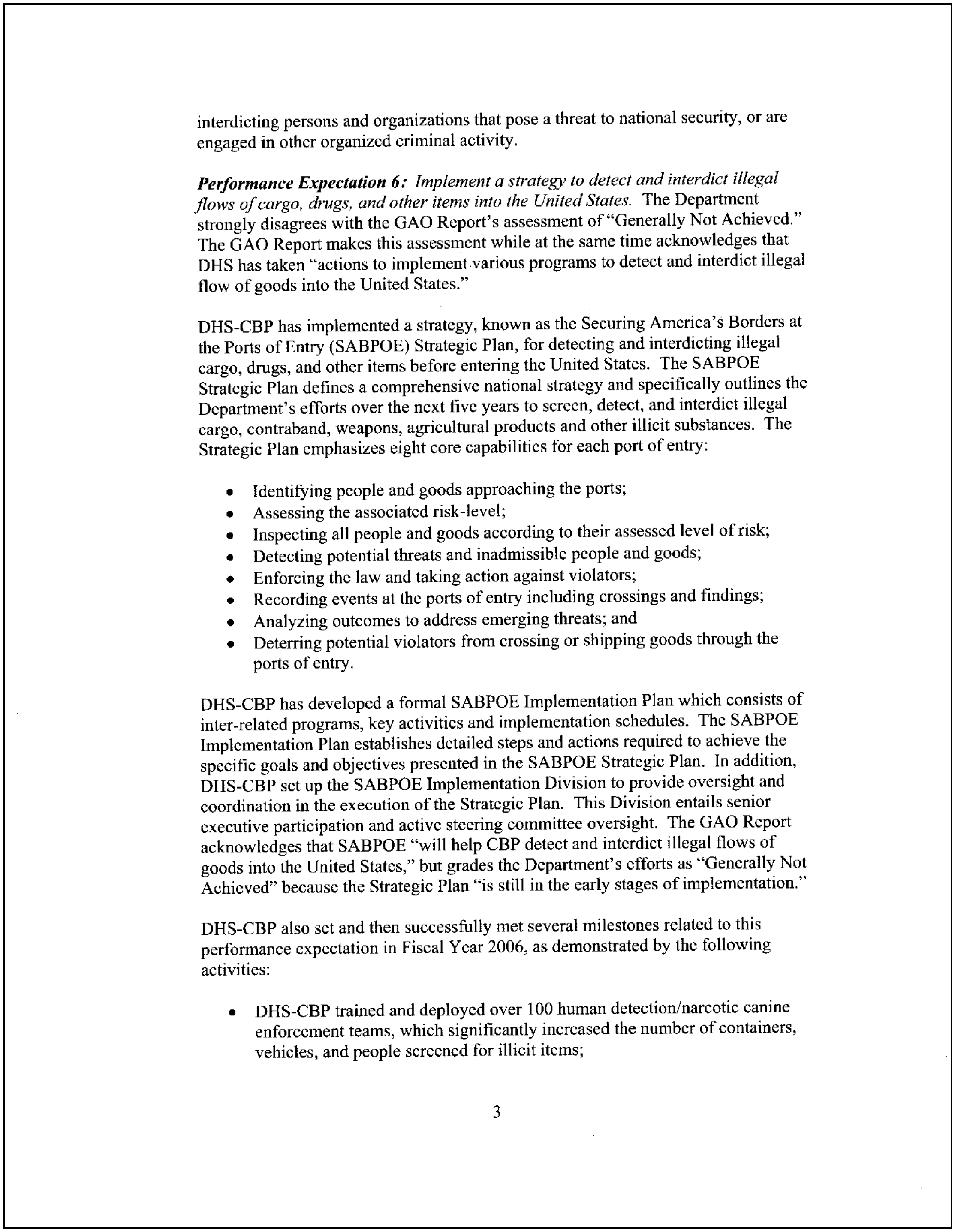


The GAO Report also justifies its assessment of "Generally Not Achieved" by asserting that the progress that has been made on the implementation of SBI*net* is "unclear." However, according to the definitions of the assessment standards repeated throughout the GAO Report, a rating of "No Assessment Made" is appropriate when "the information DHS provided did not enable [GAO] to clearly assess DHS's progress in achieving the performance expectation." Thus, it appears that GAO officials did not follow their own ratings system or were unable to do so because the standards were never sufficiently defined.

Furthermore, the GAO Report mentions, but does not adequately consider the Department's implementation of other programs and initiatives which have yielded significant results related to preventing illegal border crossings and securing the border. For example, 6,000 National Guard members were deployed to the southwest border as part of Operation Jump Start and the President's initiative to secure the border. In addition, Border Patrol agent staffing has increased by over 30 percent since 2001. Moreover, we have ended the practice of "catch and release" for other-than-Mexican apprehensions along the border. Results to date have been promising. DHS-CBP Border Patrol apprehensions for the first three quarters of Fiscal Year 2007 are down 24 percent compared to the previous year along the southwest border, indicating a significant decline in illegal cross-border activity between ports of entry. The Yuma, Arizona, and Del Rio, Texas, sectors experienced the greatest declines, with decreases of 68 percent and 51 percent, respectively. The number of other-than-Mexican alien apprehensions dropped 48 percent along the southern border. The decrease in other-than-Mexican apprehensions reduces the time agents spend transporting and processing, and increases the time spent patrolling the border.

DHS-CBP currently has effective control of 380 miles on the southwest border, plans to achieve effective control of 642 miles by the end of calendar year 2008, and anticipates having effective control over the entire southwest border by 2013. Nevertheless, the GAO Report assigns low grades to these efforts because DHS, while on target, does not yet have effective control over the more than 6,000 miles of U.S. land border.

The GAO Report also does not consider DHS-CBP efforts toward effective control over the northern border. Contrary to the GAO Report's assertion that DHS-CBP will not begin work on the northern border until fiscal year 2009, DHS-CBP has tripled the number of agents assigned to the northern border since Fiscal Year 2001. DHS-CBP recently initiated a Nationwide Voluntary Relocation Opportunity, which has brought additional, experienced agents to the U.S./Canadian border. In addition, the Department has deployed technology to provide additional coverage along the northern border – including ground sensors, cameras, radar, and sophisticated software packages. DHS-CBP implemented Border Security Evaluation Teams (BSETs) in all eight northern border sectors to secure portions of the U.S./Canadian border that were previously too remote to have been monitored. Through a partnership with the Canadian government, the Integrated Border Enforcement Team (IBET) enhances border integrity and security by identifying, investigating, and



interdicting persons and organizations that pose a threat to national security, or are engaged in other organized criminal activity.

***Performance Expectation 6:*** *Implement a strategy to detect and interdict illegal flows of cargo, drugs, and other items into the United States.* The Department strongly disagrees with the GAO Report's assessment of "Generally Not Achieved." The GAO Report makes this assessment while at the same time acknowledges that DHS has taken "actions to implement various programs to detect and interdict illegal flow of goods into the United States."

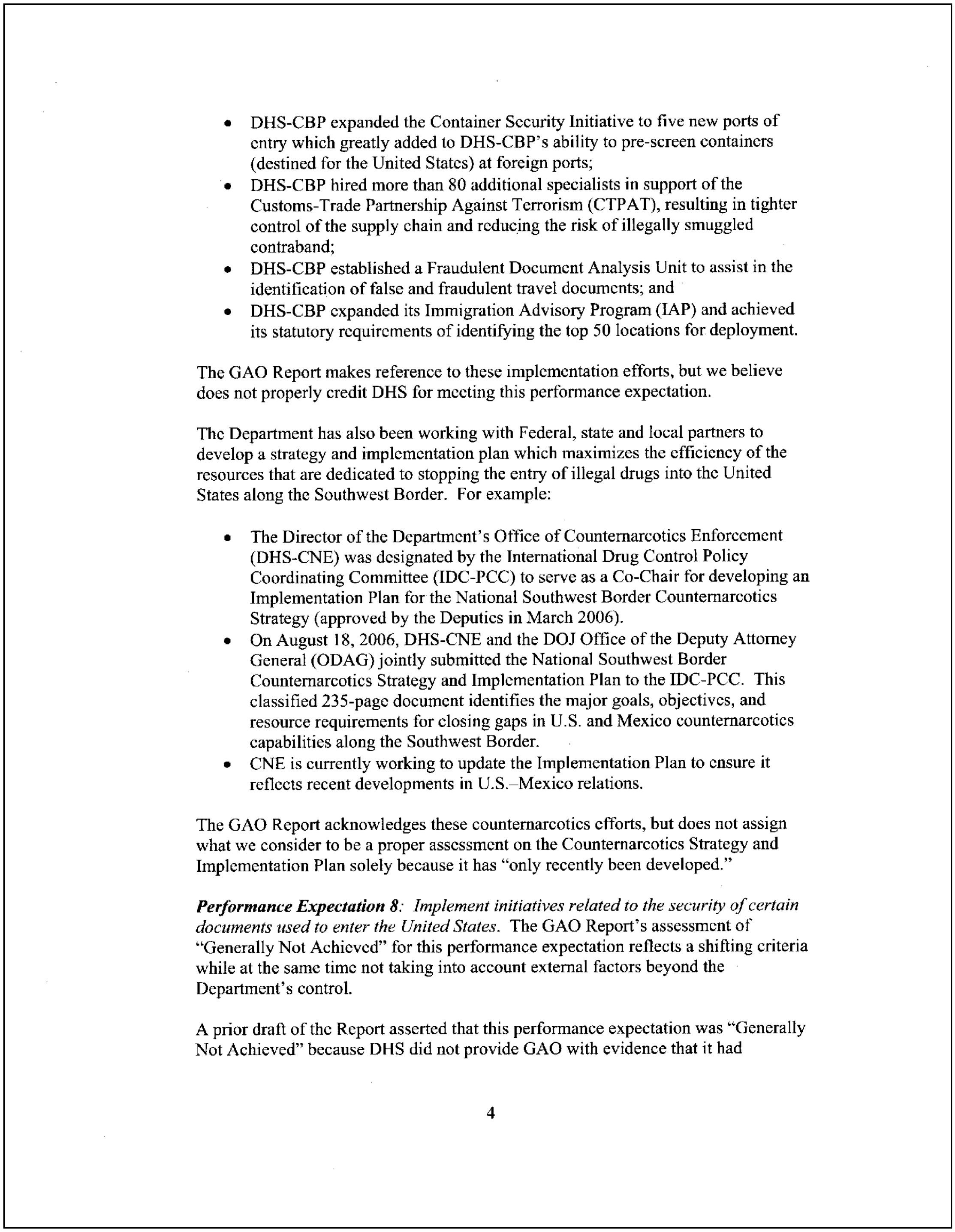
DHS-CBP has implemented a strategy, known as the Securing America's Borders at the Ports of Entry (SABPOE) Strategic Plan, for detecting and interdicting illegal cargo, drugs, and other items before entering the United States. The SABPOE Strategic Plan defines a comprehensive national strategy and specifically outlines the Department's efforts over the next five years to screen, detect, and interdict illegal cargo, contraband, weapons, agricultural products and other illicit substances. The Strategic Plan emphasizes eight core capabilities for each port of entry:

- Identifying people and goods approaching the ports;
- Assessing the associated risk-level;
- Inspecting all people and goods according to their assessed level of risk;
- Detecting potential threats and inadmissible people and goods;
- Enforcing the law and taking action against violators;
- Recording events at the ports of entry including crossings and findings;
- Analyzing outcomes to address emerging threats; and
- Deterring potential violators from crossing or shipping goods through the ports of entry.

DHS-CBP has developed a formal SABPOE Implementation Plan which consists of inter-related programs, key activities and implementation schedules. The SABPOE Implementation Plan establishes detailed steps and actions required to achieve the specific goals and objectives presented in the SABPOE Strategic Plan. In addition, DHS-CBP set up the SABPOE Implementation Division to provide oversight and coordination in the execution of the Strategic Plan. This Division entails senior executive participation and active steering committee oversight. The GAO Report acknowledges that SABPOE "will help CBP detect and interdict illegal flows of goods into the United States," but grades the Department's efforts as "Generally Not Achieved" because the Strategic Plan "is still in the early stages of implementation."

DHS-CBP also set and then successfully met several milestones related to this performance expectation in Fiscal Year 2006, as demonstrated by the following activities:

- DHS-CBP trained and deployed over 100 human detection/narcotic canine enforcement teams, which significantly increased the number of containers, vehicles, and people screened for illicit items;



- DHS-CBP expanded the Container Security Initiative to five new ports of entry which greatly added to DHS-CBP's ability to pre-screen containers (destined for the United States) at foreign ports;
- DHS-CBP hired more than 80 additional specialists in support of the Customs-Trade Partnership Against Terrorism (CTPAT), resulting in tighter control of the supply chain and reducing the risk of illegally smuggled contraband;
- DHS-CBP established a Fraudulent Document Analysis Unit to assist in the identification of false and fraudulent travel documents; and
- DHS-CBP expanded its Immigration Advisory Program (IAP) and achieved its statutory requirements of identifying the top 50 locations for deployment.

The GAO Report makes reference to these implementation efforts, but we believe does not properly credit DHS for meeting this performance expectation.

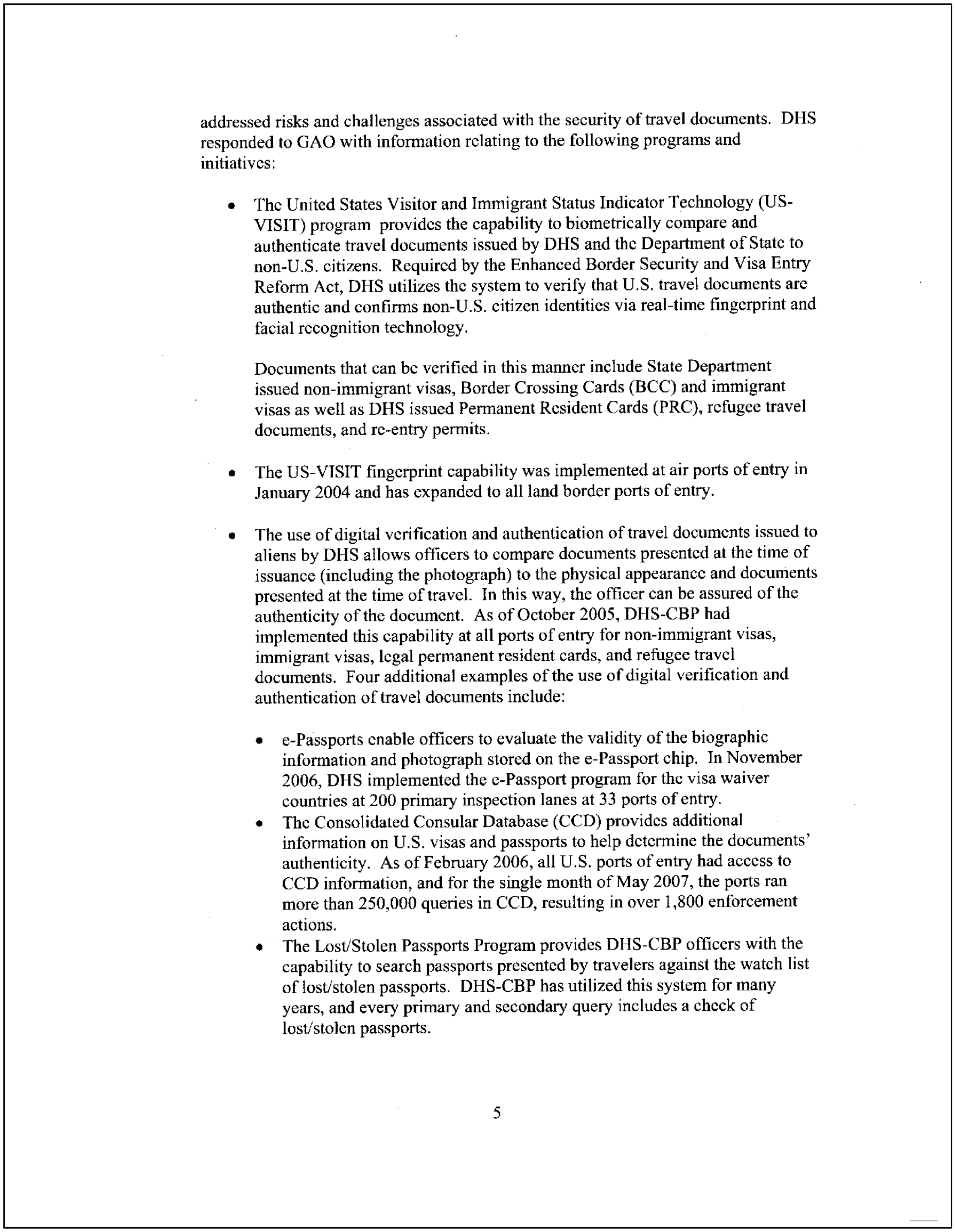
The Department has also been working with Federal, state and local partners to develop a strategy and implementation plan which maximizes the efficiency of the resources that are dedicated to stopping the entry of illegal drugs into the United States along the Southwest Border. For example:

- The Director of the Department's Office of Counternarcotics Enforcement (DHS-CNE) was designated by the International Drug Control Policy Coordinating Committee (IDC-PCC) to serve as a Co-Chair for developing an Implementation Plan for the National Southwest Border Counternarcotics Strategy (approved by the Deputies in March 2006).
- On August 18, 2006, DHS-CNE and the DOJ Office of the Deputy Attorney General (ODAG) jointly submitted the National Southwest Border Counternarcotics Strategy and Implementation Plan to the IDC-PCC. This classified 235-page document identifies the major goals, objectives, and resource requirements for closing gaps in U.S. and Mexico counternarcotics capabilities along the Southwest Border.
- CNE is currently working to update the Implementation Plan to ensure it reflects recent developments in U.S.–Mexico relations.

The GAO Report acknowledges these counternarcotics efforts, but does not assign what we consider to be a proper assessment on the Counternarcotics Strategy and Implementation Plan solely because it has "only recently been developed."

***Performance Expectation 8**: Implement initiatives related to the security of certain documents used to enter the United States.* The GAO Report's assessment of "Generally Not Achieved" for this performance expectation reflects a shifting criteria while at the same time not taking into account external factors beyond the Department's control.

A prior draft of the Report asserted that this performance expectation was "Generally Not Achieved" because DHS did not provide GAO with evidence that it had



addressed risks and challenges associated with the security of travel documents. DHS responded to GAO with information relating to the following programs and initiatives:

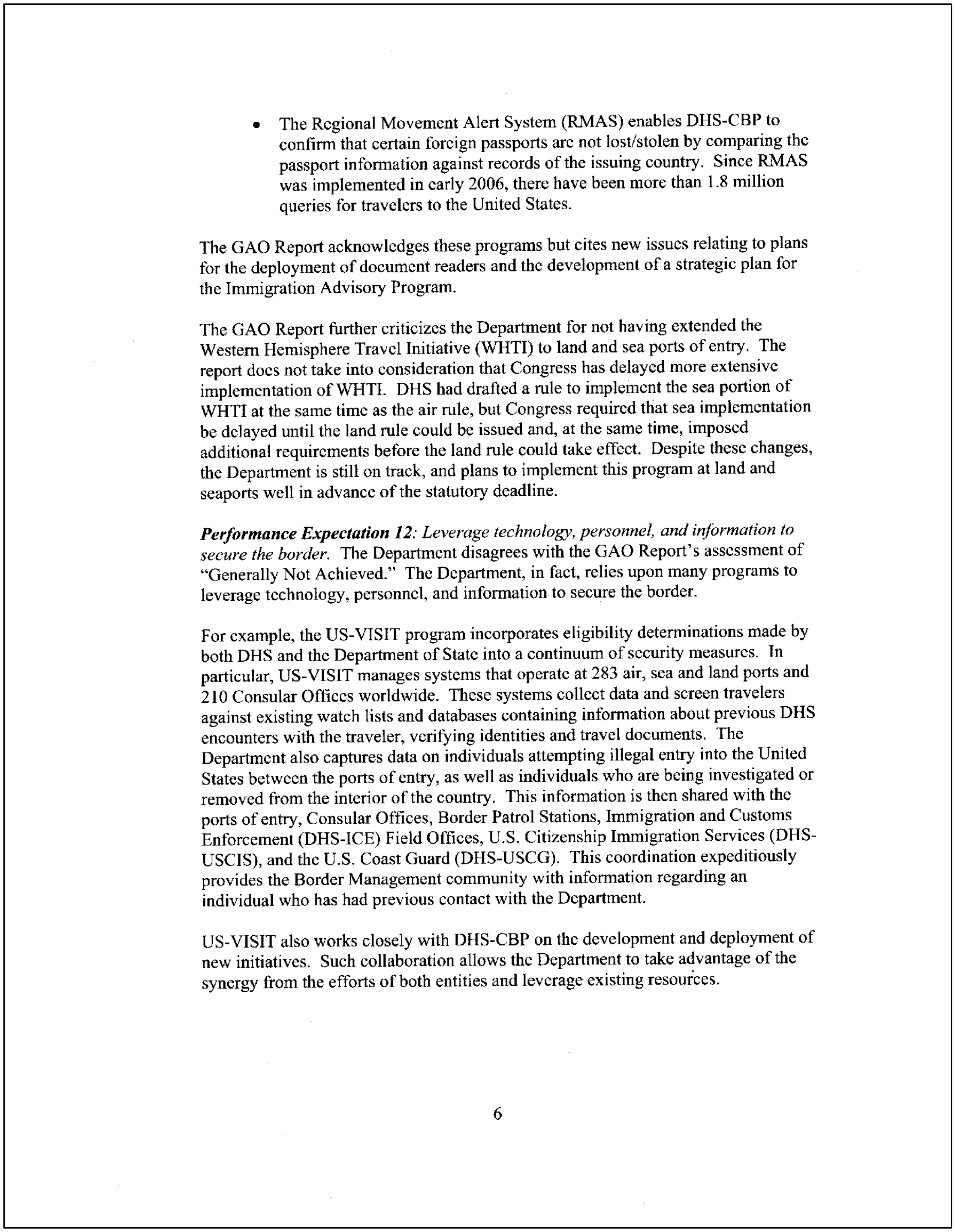
- The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program provides the capability to biometrically compare and authenticate travel documents issued by DHS and the Department of State to non-U.S. citizens. Required by the Enhanced Border Security and Visa Entry Reform Act, DHS utilizes the system to verify that U.S. travel documents are authentic and confirms non-U.S. citizen identities via real-time fingerprint and facial recognition technology.

  Documents that can be verified in this manner include State Department issued non-immigrant visas, Border Crossing Cards (BCC) and immigrant visas as well as DHS issued Permanent Resident Cards (PRC), refugee travel documents, and re-entry permits.

- The US-VISIT fingerprint capability was implemented at air ports of entry in January 2004 and has expanded to all land border ports of entry.

- The use of digital verification and authentication of travel documents issued to aliens by DHS allows officers to compare documents presented at the time of issuance (including the photograph) to the physical appearance and documents presented at the time of travel. In this way, the officer can be assured of the authenticity of the document. As of October 2005, DHS-CBP had implemented this capability at all ports of entry for non-immigrant visas, immigrant visas, legal permanent resident cards, and refugee travel documents. Four additional examples of the use of digital verification and authentication of travel documents include:

  - e-Passports enable officers to evaluate the validity of the biographic information and photograph stored on the e-Passport chip. In November 2006, DHS implemented the e-Passport program for the visa waiver countries at 200 primary inspection lanes at 33 ports of entry.
  - The Consolidated Consular Database (CCD) provides additional information on U.S. visas and passports to help determine the documents' authenticity. As of February 2006, all U.S. ports of entry had access to CCD information, and for the single month of May 2007, the ports ran more than 250,000 queries in CCD, resulting in over 1,800 enforcement actions.
  - The Lost/Stolen Passports Program provides DHS-CBP officers with the capability to search passports presented by travelers against the watch list of lost/stolen passports. DHS-CBP has utilized this system for many years, and every primary and secondary query includes a check of lost/stolen passports.



- The Regional Movement Alert System (RMAS) enables DHS-CBP to confirm that certain foreign passports are not lost/stolen by comparing the passport information against records of the issuing country. Since RMAS was implemented in early 2006, there have been more than 1.8 million queries for travelers to the United States.

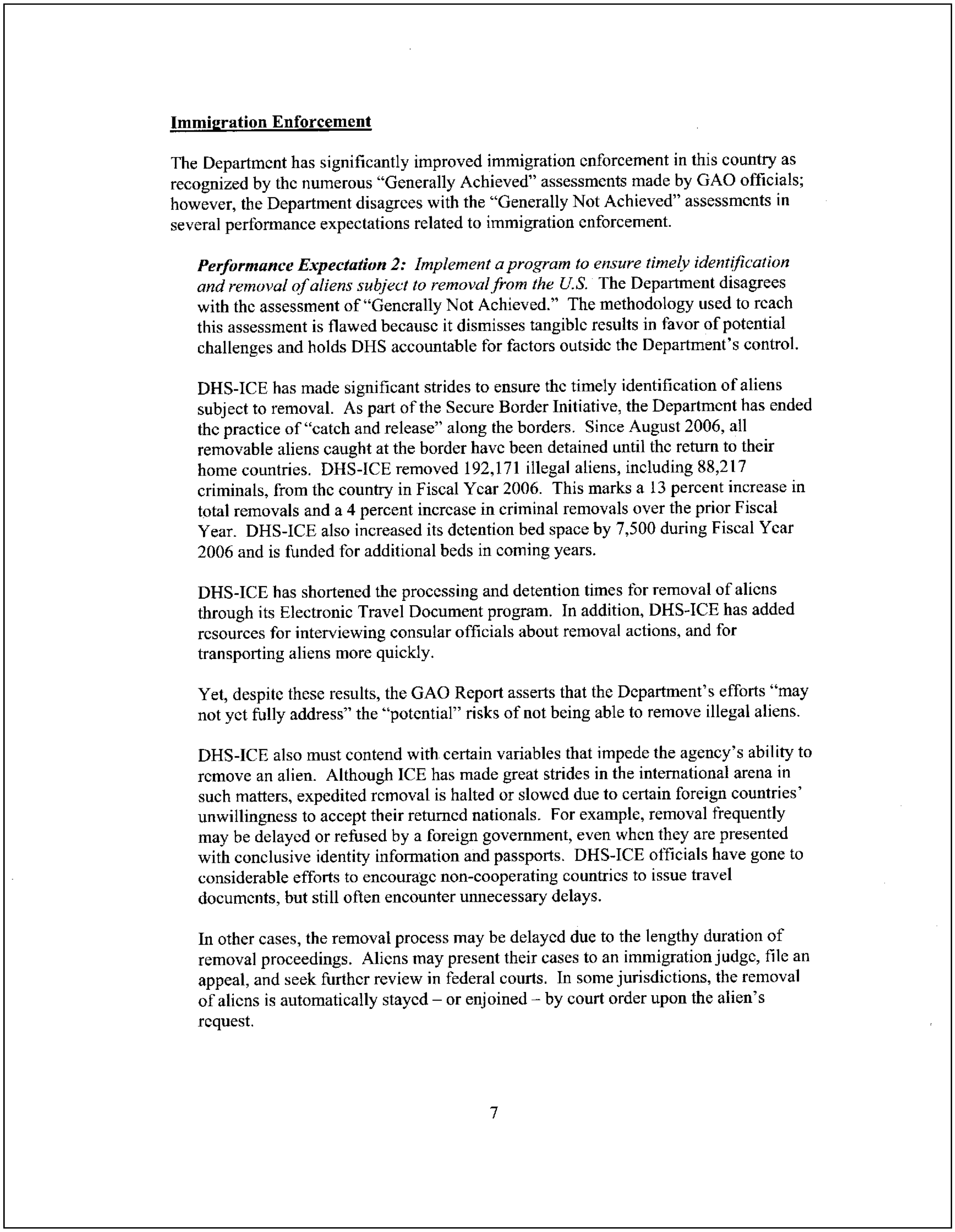
The GAO Report acknowledges these programs but cites new issues relating to plans for the deployment of document readers and the development of a strategic plan for the Immigration Advisory Program.

The GAO Report further criticizes the Department for not having extended the Western Hemisphere Travel Initiative (WHTI) to land and sea ports of entry. The report does not take into consideration that Congress has delayed more extensive implementation of WHTI. DHS had drafted a rule to implement the sea portion of WHTI at the same time as the air rule, but Congress required that sea implementation be delayed until the land rule could be issued and, at the same time, imposed additional requirements before the land rule could take effect. Despite these changes, the Department is still on track, and plans to implement this program at land and seaports well in advance of the statutory deadline.

***Performance Expectation 12****: Leverage technology, personnel, and information to secure the border.* The Department disagrees with the GAO Report's assessment of "Generally Not Achieved." The Department, in fact, relies upon many programs to leverage technology, personnel, and information to secure the border.

For example, the US-VISIT program incorporates eligibility determinations made by both DHS and the Department of State into a continuum of security measures. In particular, US-VISIT manages systems that operate at 283 air, sea and land ports and 210 Consular Offices worldwide. These systems collect data and screen travelers against existing watch lists and databases containing information about previous DHS encounters with the traveler, verifying identities and travel documents. The Department also captures data on individuals attempting illegal entry into the United States between the ports of entry, as well as individuals who are being investigated or removed from the interior of the country. This information is then shared with the ports of entry, Consular Offices, Border Patrol Stations, Immigration and Customs Enforcement (DHS-ICE) Field Offices, U.S. Citizenship Immigration Services (DHS-USCIS), and the U.S. Coast Guard (DHS-USCG). This coordination expeditiously provides the Border Management community with information regarding an individual who has had previous contact with the Department.

US-VISIT also works closely with DHS-CBP on the development and deployment of new initiatives. Such collaboration allows the Department to take advantage of the synergy from the efforts of both entities and leverage existing resources.



**Immigration Enforcement**

The Department has significantly improved immigration enforcement in this country as recognized by the numerous "Generally Achieved" assessments made by GAO officials; however, the Department disagrees with the "Generally Not Achieved" assessments in several performance expectations related to immigration enforcement.

***Performance Expectation 2:*** *Implement a program to ensure timely identification and removal of aliens subject to removal from the U.S.* The Department disagrees with the assessment of "Generally Not Achieved." The methodology used to reach this assessment is flawed because it dismisses tangible results in favor of potential challenges and holds DHS accountable for factors outside the Department's control.

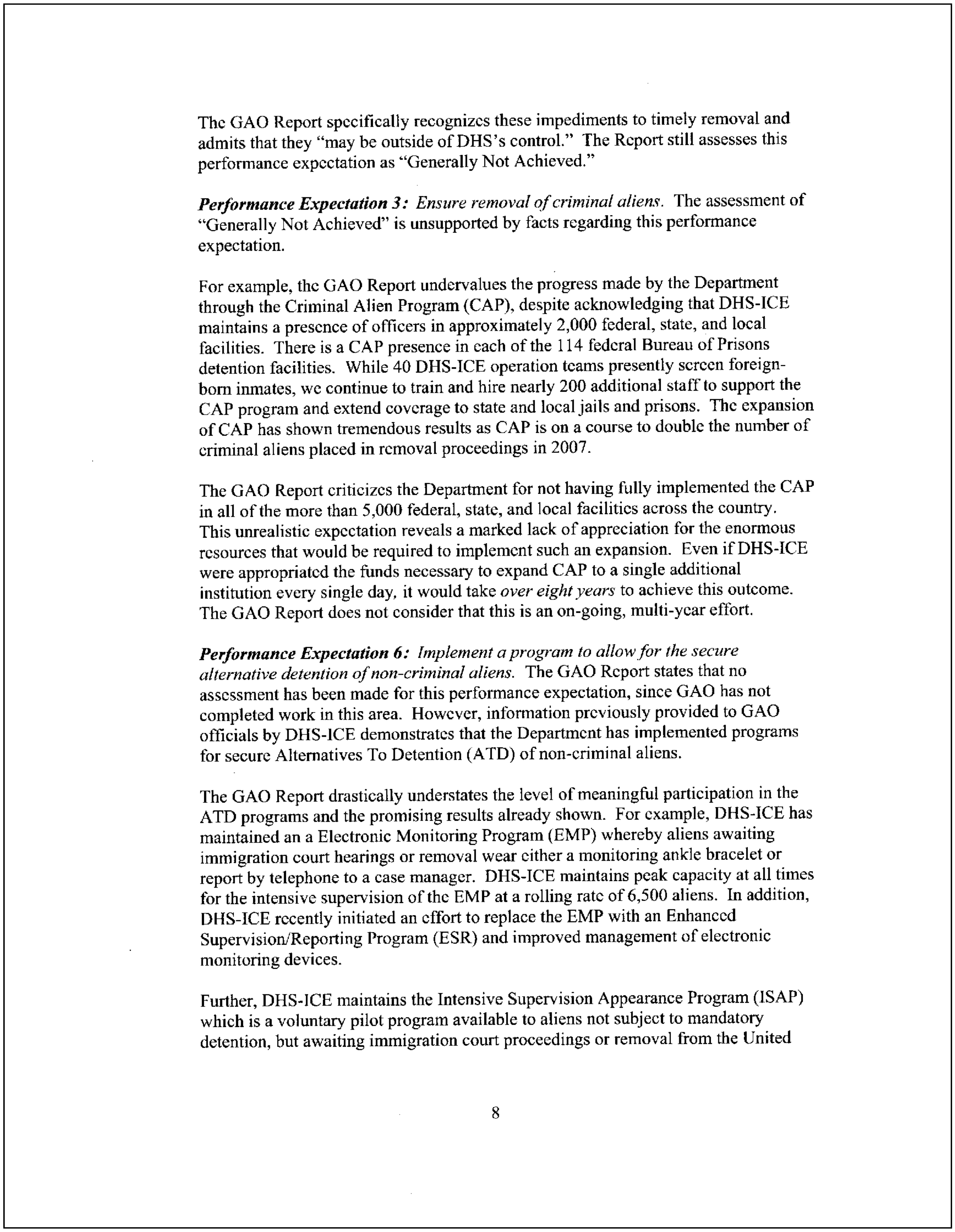
DHS-ICE has made significant strides to ensure the timely identification of aliens subject to removal. As part of the Secure Border Initiative, the Department has ended the practice of "catch and release" along the borders. Since August 2006, all removable aliens caught at the border have been detained until the return to their home countries. DHS-ICE removed 192,171 illegal aliens, including 88,217 criminals, from the country in Fiscal Year 2006. This marks a 13 percent increase in total removals and a 4 percent increase in criminal removals over the prior Fiscal Year. DHS-ICE also increased its detention bed space by 7,500 during Fiscal Year 2006 and is funded for additional beds in coming years.

DHS-ICE has shortened the processing and detention times for removal of aliens through its Electronic Travel Document program. In addition, DHS-ICE has added resources for interviewing consular officials about removal actions, and for transporting aliens more quickly.

Yet, despite these results, the GAO Report asserts that the Department's efforts "may not yet fully address" the "potential" risks of not being able to remove illegal aliens.

DHS-ICE also must contend with certain variables that impede the agency's ability to remove an alien. Although ICE has made great strides in the international arena in such matters, expedited removal is halted or slowed due to certain foreign countries' unwillingness to accept their returned nationals. For example, removal frequently may be delayed or refused by a foreign government, even when they are presented with conclusive identity information and passports. DHS-ICE officials have gone to considerable efforts to encourage non-cooperating countries to issue travel documents, but still often encounter unnecessary delays.

In other cases, the removal process may be delayed due to the lengthy duration of removal proceedings. Aliens may present their cases to an immigration judge, file an appeal, and seek further review in federal courts. In some jurisdictions, the removal of aliens is automatically stayed – or enjoined – by court order upon the alien's request.



The GAO Report specifically recognizes these impediments to timely removal and admits that they "may be outside of DHS's control." The Report still assesses this performance expectation as "Generally Not Achieved."

***Performance Expectation 3:*** *Ensure removal of criminal aliens.* The assessment of "Generally Not Achieved" is unsupported by facts regarding this performance expectation.

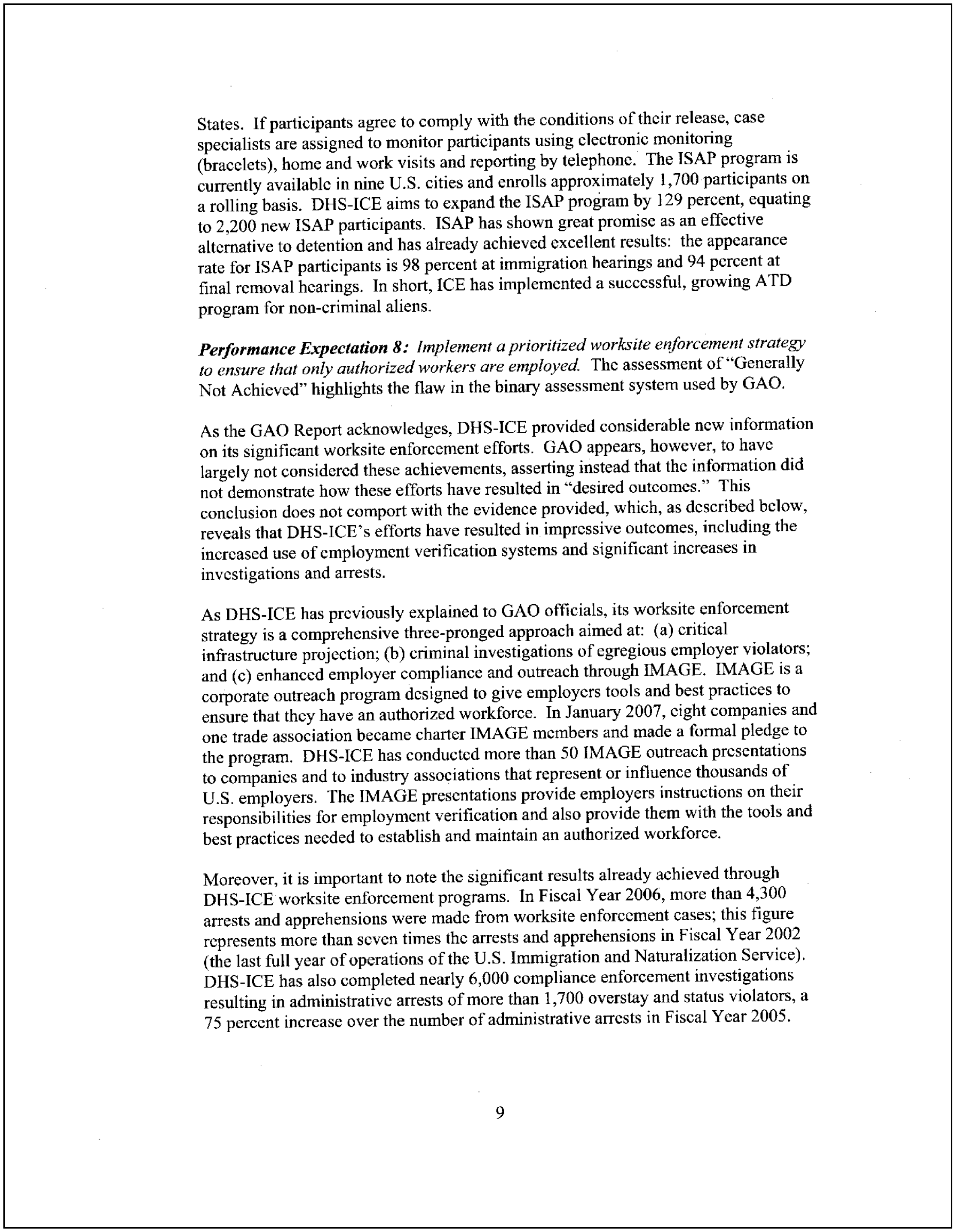
For example, the GAO Report undervalues the progress made by the Department through the Criminal Alien Program (CAP), despite acknowledging that DHS-ICE maintains a presence of officers in approximately 2,000 federal, state, and local facilities. There is a CAP presence in each of the 114 federal Bureau of Prisons detention facilities. While 40 DHS-ICE operation teams presently screen foreign-born inmates, we continue to train and hire nearly 200 additional staff to support the CAP program and extend coverage to state and local jails and prisons. The expansion of CAP has shown tremendous results as CAP is on a course to double the number of criminal aliens placed in removal proceedings in 2007.

The GAO Report criticizes the Department for not having fully implemented the CAP in all of the more than 5,000 federal, state, and local facilities across the country. This unrealistic expectation reveals a marked lack of appreciation for the enormous resources that would be required to implement such an expansion. Even if DHS-ICE were appropriated the funds necessary to expand CAP to a single additional institution every single day, it would take *over eight years* to achieve this outcome. The GAO Report does not consider that this is an on-going, multi-year effort.

***Performance Expectation 6:*** *Implement a program to allow for the secure alternative detention of non-criminal aliens.* The GAO Report states that no assessment has been made for this performance expectation, since GAO has not completed work in this area. However, information previously provided to GAO officials by DHS-ICE demonstrates that the Department has implemented programs for secure Alternatives To Detention (ATD) of non-criminal aliens.

The GAO Report drastically understates the level of meaningful participation in the ATD programs and the promising results already shown. For example, DHS-ICE has maintained an a Electronic Monitoring Program (EMP) whereby aliens awaiting immigration court hearings or removal wear either a monitoring ankle bracelet or report by telephone to a case manager. DHS-ICE maintains peak capacity at all times for the intensive supervision of the EMP at a rolling rate of 6,500 aliens. In addition, DHS-ICE recently initiated an effort to replace the EMP with an Enhanced Supervision/Reporting Program (ESR) and improved management of electronic monitoring devices.

Further, DHS-ICE maintains the Intensive Supervision Appearance Program (ISAP) which is a voluntary pilot program available to aliens not subject to mandatory detention, but awaiting immigration court proceedings or removal from the United



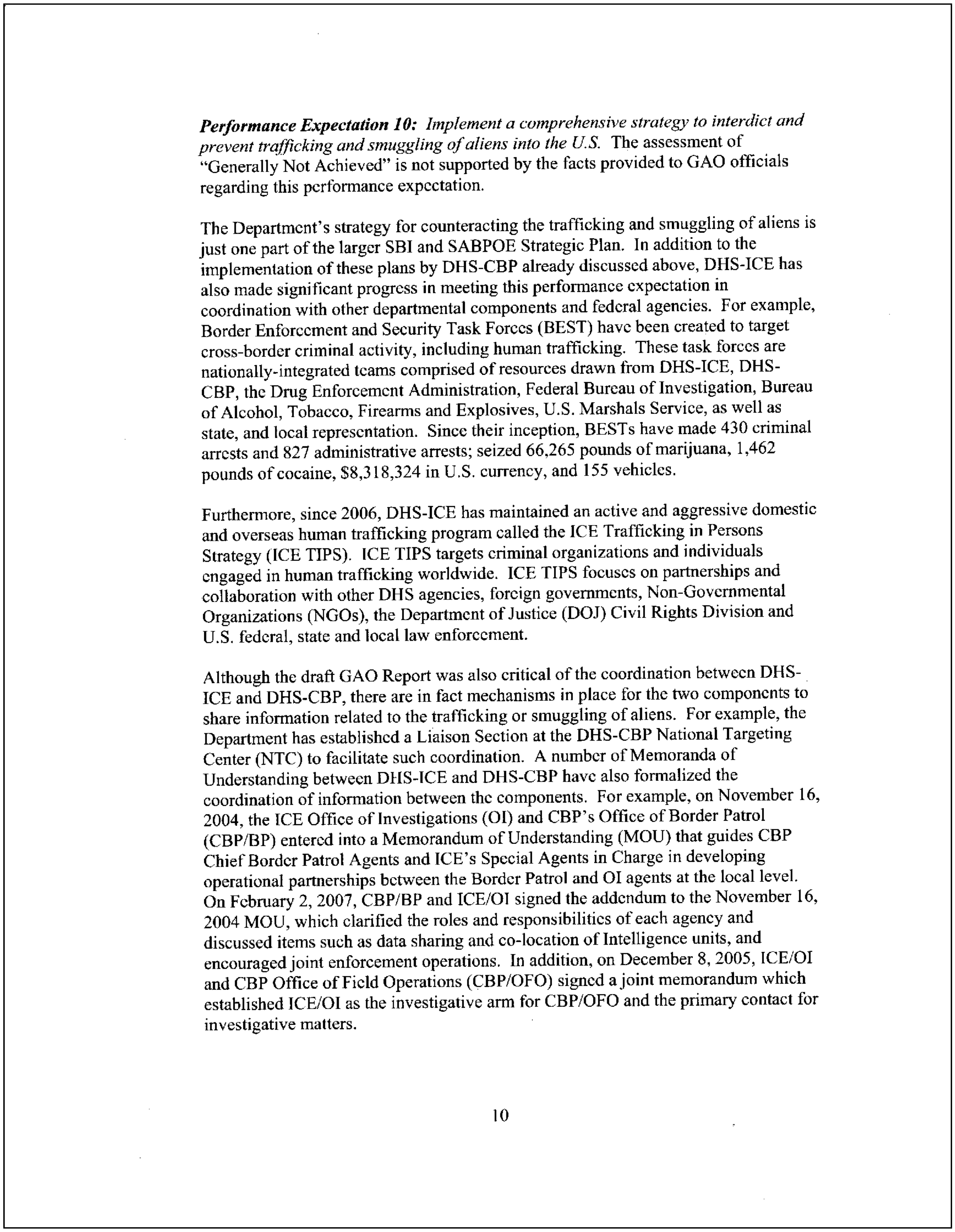
States. If participants agree to comply with the conditions of their release, case specialists are assigned to monitor participants using electronic monitoring (bracelets), home and work visits and reporting by telephone. The ISAP program is currently available in nine U.S. cities and enrolls approximately 1,700 participants on a rolling basis. DHS-ICE aims to expand the ISAP program by 129 percent, equating to 2,200 new ISAP participants. ISAP has shown great promise as an effective alternative to detention and has already achieved excellent results: the appearance rate for ISAP participants is 98 percent at immigration hearings and 94 percent at final removal hearings. In short, ICE has implemented a successful, growing ATD program for non-criminal aliens.

***Performance Expectation 8:*** *Implement a prioritized worksite enforcement strategy to ensure that only authorized workers are employed.* The assessment of "Generally Not Achieved" highlights the flaw in the binary assessment system used by GAO.

As the GAO Report acknowledges, DHS-ICE provided considerable new information on its significant worksite enforcement efforts. GAO appears, however, to have largely not considered these achievements, asserting instead that the information did not demonstrate how these efforts have resulted in "desired outcomes." This conclusion does not comport with the evidence provided, which, as described below, reveals that DHS-ICE's efforts have resulted in impressive outcomes, including the increased use of employment verification systems and significant increases in investigations and arrests.

As DHS-ICE has previously explained to GAO officials, its worksite enforcement strategy is a comprehensive three-pronged approach aimed at: (a) critical infrastructure projection; (b) criminal investigations of egregious employer violators; and (c) enhanced employer compliance and outreach through IMAGE. IMAGE is a corporate outreach program designed to give employers tools and best practices to ensure that they have an authorized workforce. In January 2007, eight companies and one trade association became charter IMAGE members and made a formal pledge to the program. DHS-ICE has conducted more than 50 IMAGE outreach presentations to companies and to industry associations that represent or influence thousands of U.S. employers. The IMAGE presentations provide employers instructions on their responsibilities for employment verification and also provide them with the tools and best practices needed to establish and maintain an authorized workforce.

Moreover, it is important to note the significant results already achieved through DHS-ICE worksite enforcement programs. In Fiscal Year 2006, more than 4,300 arrests and apprehensions were made from worksite enforcement cases; this figure represents more than seven times the arrests and apprehensions in Fiscal Year 2002 (the last full year of operations of the U.S. Immigration and Naturalization Service). DHS-ICE has also completed nearly 6,000 compliance enforcement investigations resulting in administrative arrests of more than 1,700 overstay and status violators, a 75 percent increase over the number of administrative arrests in Fiscal Year 2005.

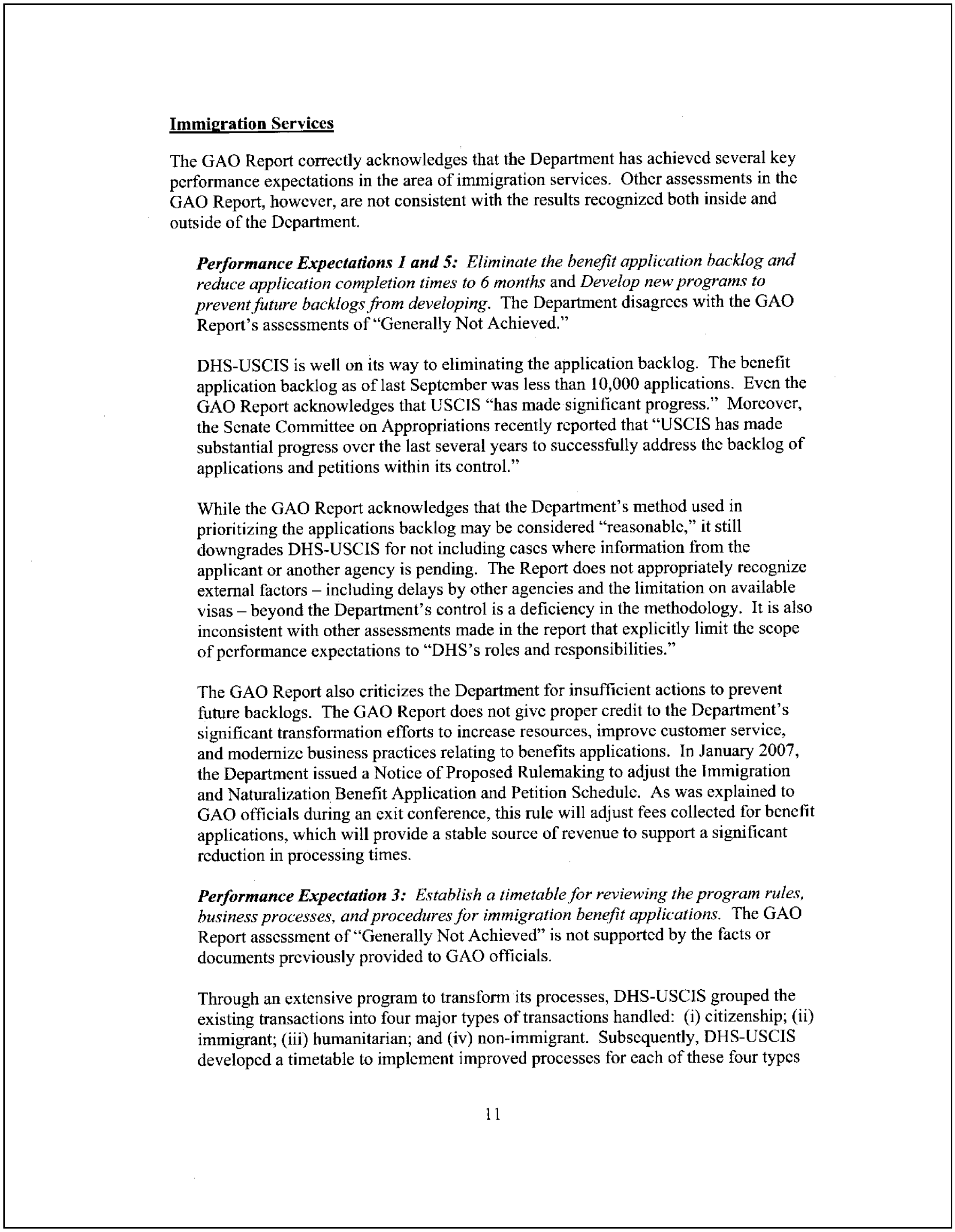


***Performance Expectation 10:*** *Implement a comprehensive strategy to interdict and prevent trafficking and smuggling of aliens into the U.S.* The assessment of "Generally Not Achieved" is not supported by the facts provided to GAO officials regarding this performance expectation.

The Department's strategy for counteracting the trafficking and smuggling of aliens is just one part of the larger SBI and SABPOE Strategic Plan. In addition to the implementation of these plans by DHS-CBP already discussed above, DHS-ICE has also made significant progress in meeting this performance expectation in coordination with other departmental components and federal agencies. For example, Border Enforcement and Security Task Forces (BEST) have been created to target cross-border criminal activity, including human trafficking. These task forces are nationally-integrated teams comprised of resources drawn from DHS-ICE, DHS-CBP, the Drug Enforcement Administration, Federal Bureau of Investigation, Bureau of Alcohol, Tobacco, Firearms and Explosives, U.S. Marshals Service, as well as state, and local representation. Since their inception, BESTs have made 430 criminal arrests and 827 administrative arrests; seized 66,265 pounds of marijuana, 1,462 pounds of cocaine, $8,318,324 in U.S. currency, and 155 vehicles.

Furthermore, since 2006, DHS-ICE has maintained an active and aggressive domestic and overseas human trafficking program called the ICE Trafficking in Persons Strategy (ICE TIPS). ICE TIPS targets criminal organizations and individuals engaged in human trafficking worldwide. ICE TIPS focuses on partnerships and collaboration with other DHS agencies, foreign governments, Non-Governmental Organizations (NGOs), the Department of Justice (DOJ) Civil Rights Division and U.S. federal, state and local law enforcement.

Although the draft GAO Report was also critical of the coordination between DHS-ICE and DHS-CBP, there are in fact mechanisms in place for the two components to share information related to the trafficking or smuggling of aliens. For example, the Department has established a Liaison Section at the DHS-CBP National Targeting Center (NTC) to facilitate such coordination. A number of Memoranda of Understanding between DHS-ICE and DHS-CBP have also formalized the coordination of information between the components. For example, on November 16, 2004, the ICE Office of Investigations (OI) and CBP's Office of Border Patrol (CBP/BP) entered into a Memorandum of Understanding (MOU) that guides CBP Chief Border Patrol Agents and ICE's Special Agents in Charge in developing operational partnerships between the Border Patrol and OI agents at the local level. On February 2, 2007, CBP/BP and ICE/OI signed the addendum to the November 16, 2004 MOU, which clarified the roles and responsibilities of each agency and discussed items such as data sharing and co-location of Intelligence units, and encouraged joint enforcement operations. In addition, on December 8, 2005, ICE/OI and CBP Office of Field Operations (CBP/OFO) signed a joint memorandum which established ICE/OI as the investigative arm for CBP/OFO and the primary contact for investigative matters.



**Immigration Services**

The GAO Report correctly acknowledges that the Department has achieved several key performance expectations in the area of immigration services. Other assessments in the GAO Report, however, are not consistent with the results recognized both inside and outside of the Department.

***Performance Expectations 1 and 5:*** *Eliminate the benefit application backlog and reduce application completion times to 6 months* and *Develop new programs to prevent future backlogs from developing.* The Department disagrees with the GAO Report's assessments of "Generally Not Achieved."

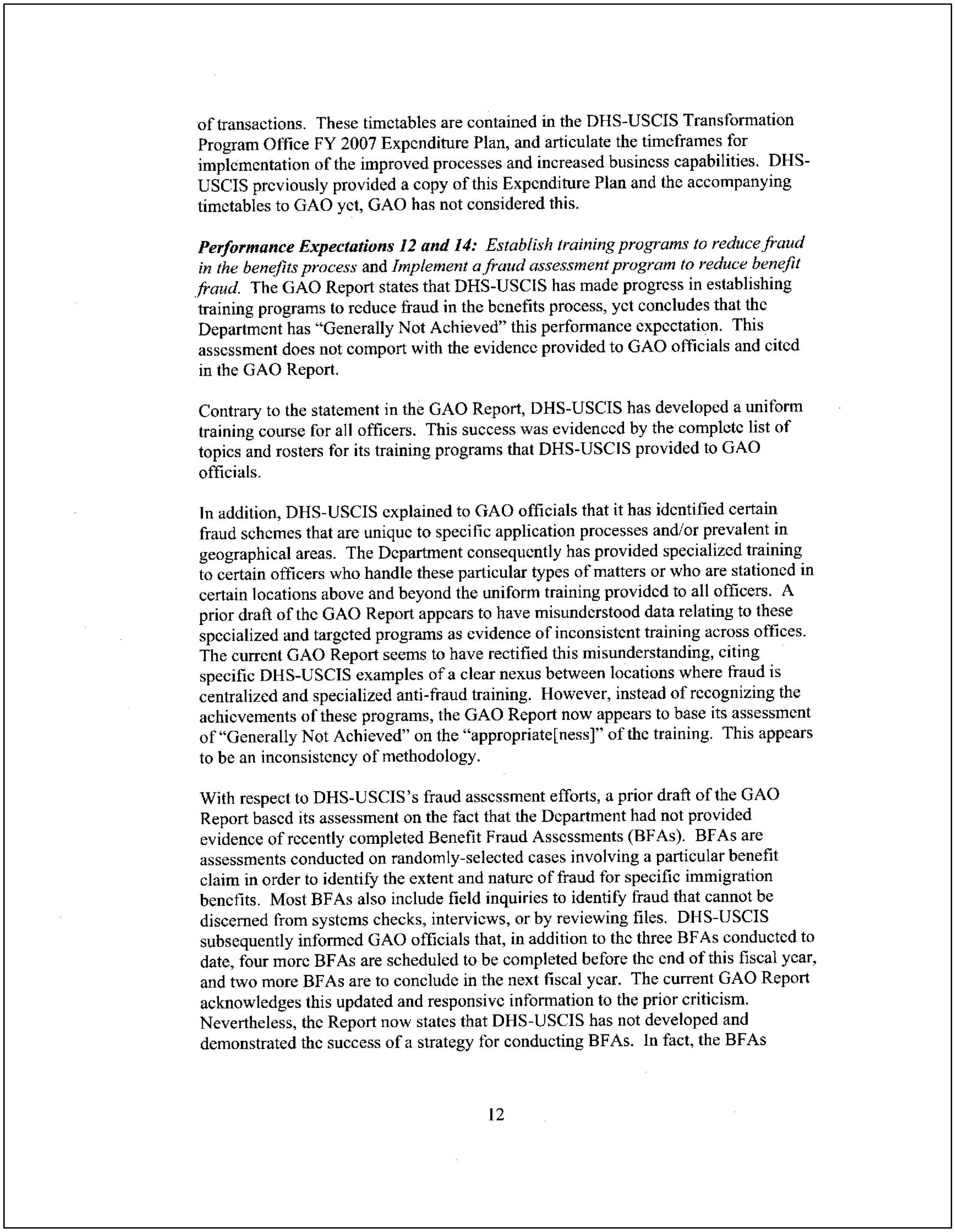
DHS-USCIS is well on its way to eliminating the application backlog. The benefit application backlog as of last September was less than 10,000 applications. Even the GAO Report acknowledges that USCIS "has made significant progress." Moreover, the Senate Committee on Appropriations recently reported that "USCIS has made substantial progress over the last several years to successfully address the backlog of applications and petitions within its control."

While the GAO Report acknowledges that the Department's method used in prioritizing the applications backlog may be considered "reasonable," it still downgrades DHS-USCIS for not including cases where information from the applicant or another agency is pending. The Report does not appropriately recognize external factors – including delays by other agencies and the limitation on available visas – beyond the Department's control is a deficiency in the methodology. It is also inconsistent with other assessments made in the report that explicitly limit the scope of performance expectations to "DHS's roles and responsibilities."

The GAO Report also criticizes the Department for insufficient actions to prevent future backlogs. The GAO Report does not give proper credit to the Department's significant transformation efforts to increase resources, improve customer service, and modernize business practices relating to benefits applications. In January 2007, the Department issued a Notice of Proposed Rulemaking to adjust the Immigration and Naturalization Benefit Application and Petition Schedule. As was explained to GAO officials during an exit conference, this rule will adjust fees collected for benefit applications, which will provide a stable source of revenue to support a significant reduction in processing times.

***Performance Expectation 3:*** *Establish a timetable for reviewing the program rules, business processes, and procedures for immigration benefit applications.* The GAO Report assessment of "Generally Not Achieved" is not supported by the facts or documents previously provided to GAO officials.

Through an extensive program to transform its processes, DHS-USCIS grouped the existing transactions into four major types of transactions handled: (i) citizenship; (ii) immigrant; (iii) humanitarian; and (iv) non-immigrant. Subsequently, DHS-USCIS developed a timetable to implement improved processes for each of these four types



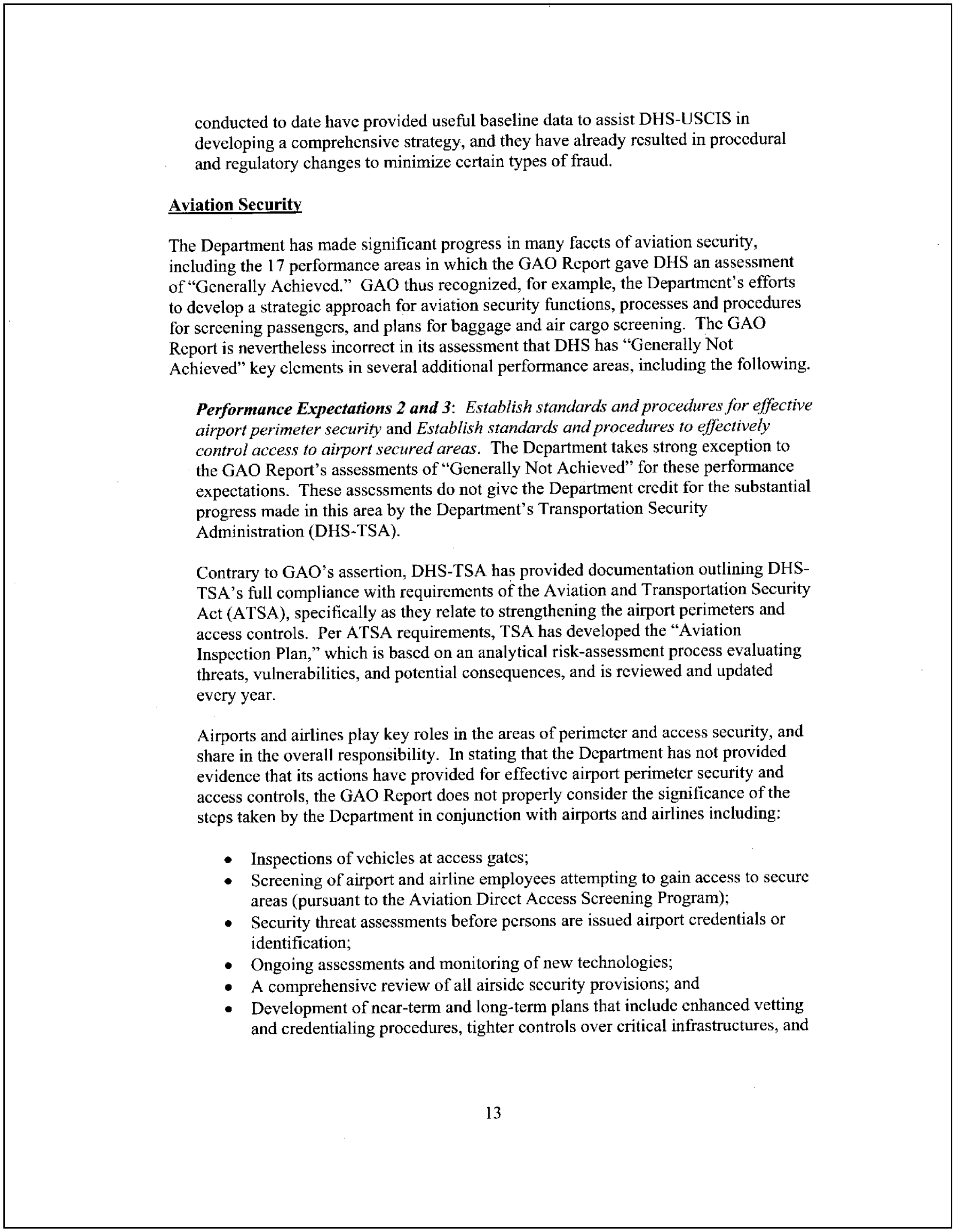
of transactions. These timetables are contained in the DHS-USCIS Transformation Program Office FY 2007 Expenditure Plan, and articulate the timeframes for implementation of the improved processes and increased business capabilities. DHS-USCIS previously provided a copy of this Expenditure Plan and the accompanying timetables to GAO yet, GAO has not considered this.

***Performance Expectations 12 and 14:*** *Establish training programs to reduce fraud in the benefits process* and *Implement a fraud assessment program to reduce benefit fraud.* The GAO Report states that DHS-USCIS has made progress in establishing training programs to reduce fraud in the benefits process, yet concludes that the Department has "Generally Not Achieved" this performance expectation. This assessment does not comport with the evidence provided to GAO officials and cited in the GAO Report.

Contrary to the statement in the GAO Report, DHS-USCIS has developed a uniform training course for all officers. This success was evidenced by the complete list of topics and rosters for its training programs that DHS-USCIS provided to GAO officials.

In addition, DHS-USCIS explained to GAO officials that it has identified certain fraud schemes that are unique to specific application processes and/or prevalent in geographical areas. The Department consequently has provided specialized training to certain officers who handle these particular types of matters or who are stationed in certain locations above and beyond the uniform training provided to all officers. A prior draft of the GAO Report appears to have misunderstood data relating to these specialized and targeted programs as evidence of inconsistent training across offices. The current GAO Report seems to have rectified this misunderstanding, citing specific DHS-USCIS examples of a clear nexus between locations where fraud is centralized and specialized anti-fraud training. However, instead of recognizing the achievements of these programs, the GAO Report now appears to base its assessment of "Generally Not Achieved" on the "appropriate[ness]" of the training. This appears to be an inconsistency of methodology.

With respect to DHS-USCIS's fraud assessment efforts, a prior draft of the GAO Report based its assessment on the fact that the Department had not provided evidence of recently completed Benefit Fraud Assessments (BFAs). BFAs are assessments conducted on randomly-selected cases involving a particular benefit claim in order to identify the extent and nature of fraud for specific immigration benefits. Most BFAs also include field inquiries to identify fraud that cannot be discerned from systems checks, interviews, or by reviewing files. DHS-USCIS subsequently informed GAO officials that, in addition to the three BFAs conducted to date, four more BFAs are scheduled to be completed before the end of this fiscal year, and two more BFAs are to conclude in the next fiscal year. The current GAO Report acknowledges this updated and responsive information to the prior criticism. Nevertheless, the Report now states that DHS-USCIS has not developed and demonstrated the success of a strategy for conducting BFAs. In fact, the BFAs



conducted to date have provided useful baseline data to assist DHS-USCIS in developing a comprehensive strategy, and they have already resulted in procedural and regulatory changes to minimize certain types of fraud.

**Aviation Security**

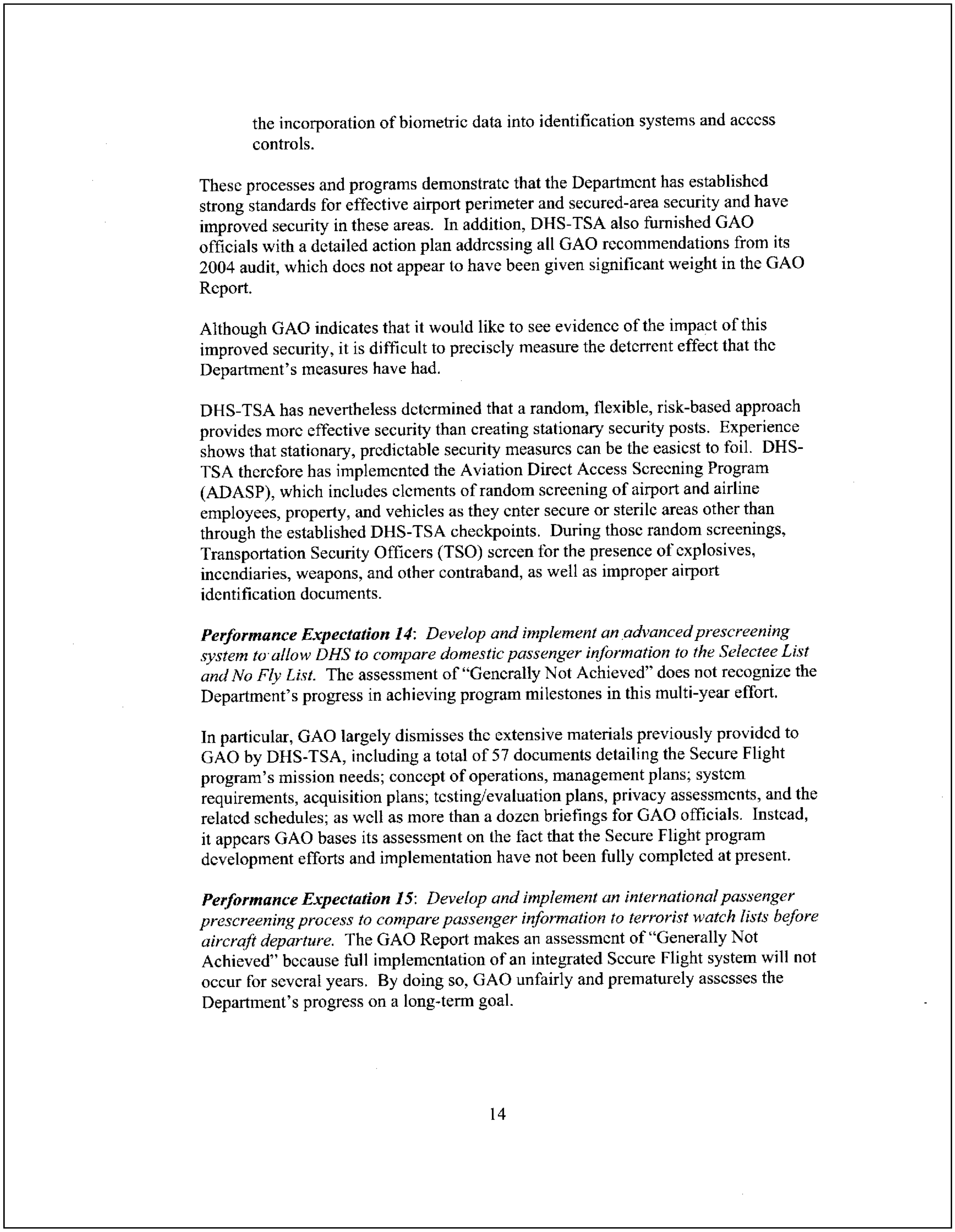
The Department has made significant progress in many facets of aviation security, including the 17 performance areas in which the GAO Report gave DHS an assessment of "Generally Achieved." GAO thus recognized, for example, the Department's efforts to develop a strategic approach for aviation security functions, processes and procedures for screening passengers, and plans for baggage and air cargo screening. The GAO Report is nevertheless incorrect in its assessment that DHS has "Generally Not Achieved" key elements in several additional performance areas, including the following.

***Performance Expectations 2 and 3***: *Establish standards and procedures for effective airport perimeter security* and *Establish standards and procedures to effectively control access to airport secured areas.* The Department takes strong exception to the GAO Report's assessments of "Generally Not Achieved" for these performance expectations. These assessments do not give the Department credit for the substantial progress made in this area by the Department's Transportation Security Administration (DHS-TSA).

Contrary to GAO's assertion, DHS-TSA has provided documentation outlining DHS-TSA's full compliance with requirements of the Aviation and Transportation Security Act (ATSA), specifically as they relate to strengthening the airport perimeters and access controls. Per ATSA requirements, TSA has developed the "Aviation Inspection Plan," which is based on an analytical risk-assessment process evaluating threats, vulnerabilities, and potential consequences, and is reviewed and updated every year.

Airports and airlines play key roles in the areas of perimeter and access security, and share in the overall responsibility. In stating that the Department has not provided evidence that its actions have provided for effective airport perimeter security and access controls, the GAO Report does not properly consider the significance of the steps taken by the Department in conjunction with airports and airlines including:

- Inspections of vehicles at access gates;
- Screening of airport and airline employees attempting to gain access to secure areas (pursuant to the Aviation Direct Access Screening Program);
- Security threat assessments before persons are issued airport credentials or identification;
- Ongoing assessments and monitoring of new technologies;
- A comprehensive review of all airside security provisions; and
- Development of near-term and long-term plans that include enhanced vetting and credentialing procedures, tighter controls over critical infrastructures, and



the incorporation of biometric data into identification systems and access controls.

These processes and programs demonstrate that the Department has established strong standards for effective airport perimeter and secured-area security and have improved security in these areas. In addition, DHS-TSA also furnished GAO officials with a detailed action plan addressing all GAO recommendations from its 2004 audit, which does not appear to have been given significant weight in the GAO Report.

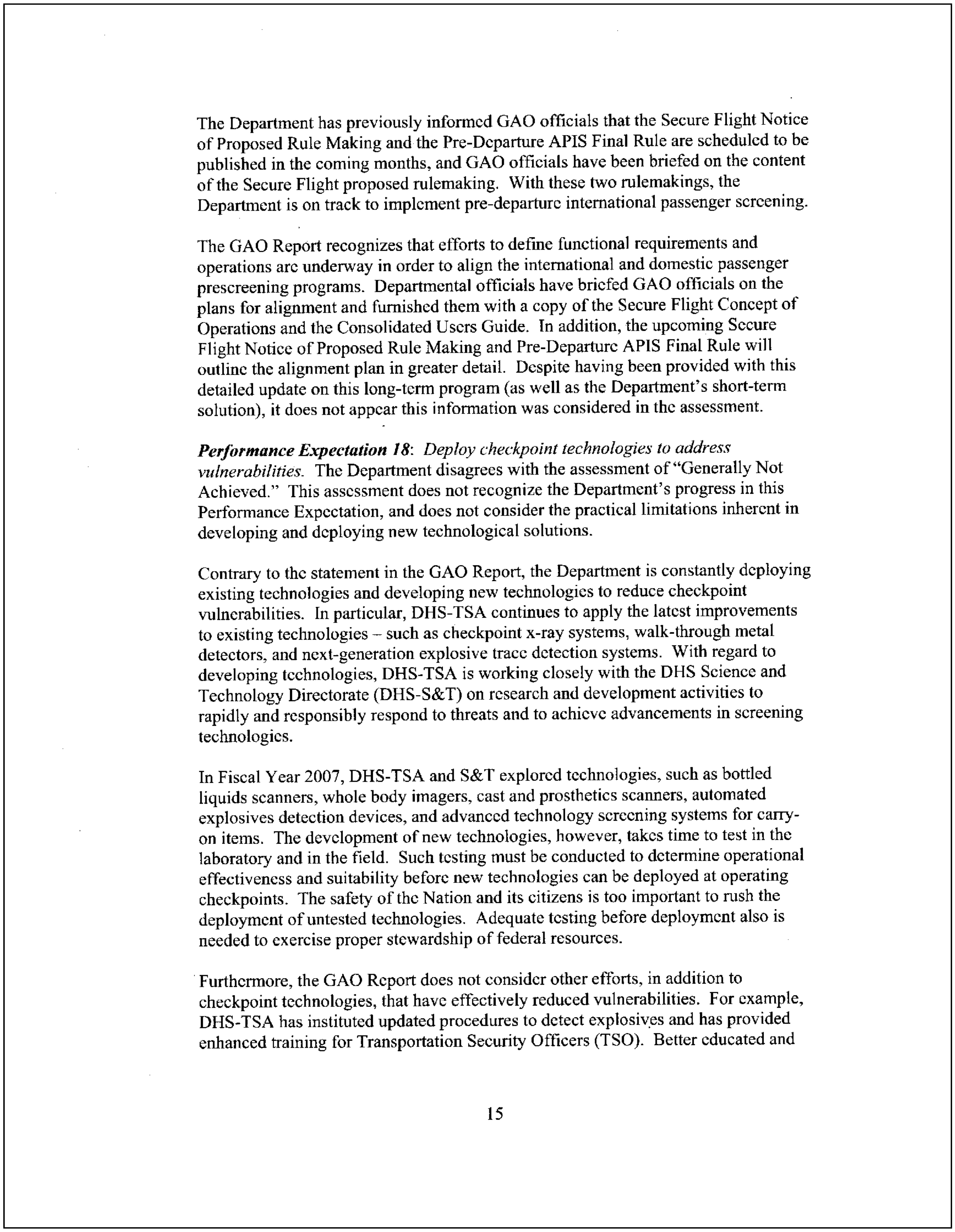
Although GAO indicates that it would like to see evidence of the impact of this improved security, it is difficult to precisely measure the deterrent effect that the Department's measures have had.

DHS-TSA has nevertheless determined that a random, flexible, risk-based approach provides more effective security than creating stationary security posts. Experience shows that stationary, predictable security measures can be the easiest to foil. DHS-TSA therefore has implemented the Aviation Direct Access Screening Program (ADASP), which includes elements of random screening of airport and airline employees, property, and vehicles as they enter secure or sterile areas other than through the established DHS-TSA checkpoints. During those random screenings, Transportation Security Officers (TSO) screen for the presence of explosives, incendiaries, weapons, and other contraband, as well as improper airport identification documents.

***Performance Expectation 14***: *Develop and implement an advanced prescreening system to allow DHS to compare domestic passenger information to the Selectee List and No Fly List.* The assessment of "Generally Not Achieved" does not recognize the Department's progress in achieving program milestones in this multi-year effort.

In particular, GAO largely dismisses the extensive materials previously provided to GAO by DHS-TSA, including a total of 57 documents detailing the Secure Flight program's mission needs; concept of operations, management plans; system requirements, acquisition plans; testing/evaluation plans, privacy assessments, and the related schedules; as well as more than a dozen briefings for GAO officials. Instead, it appears GAO bases its assessment on the fact that the Secure Flight program development efforts and implementation have not been fully completed at present.

***Performance Expectation 15***: *Develop and implement an international passenger prescreening process to compare passenger information to terrorist watch lists before aircraft departure.* The GAO Report makes an assessment of "Generally Not Achieved" because full implementation of an integrated Secure Flight system will not occur for several years. By doing so, GAO unfairly and prematurely assesses the Department's progress on a long-term goal.



The Department has previously informed GAO officials that the Secure Flight Notice of Proposed Rule Making and the Pre-Departure APIS Final Rule are scheduled to be published in the coming months, and GAO officials have been briefed on the content of the Secure Flight proposed rulemaking. With these two rulemakings, the Department is on track to implement pre-departure international passenger screening.

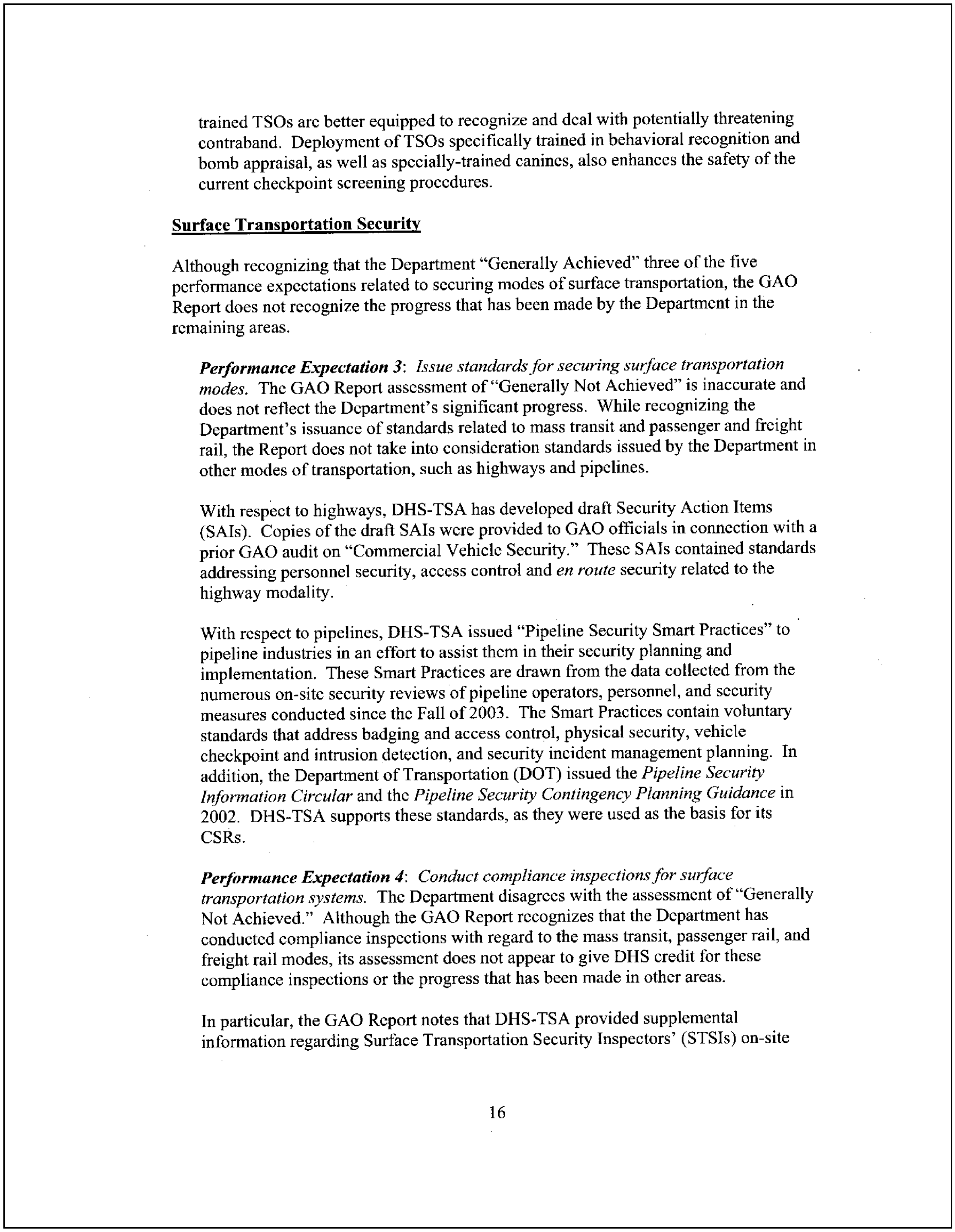
The GAO Report recognizes that efforts to define functional requirements and operations are underway in order to align the international and domestic passenger prescreening programs. Departmental officials have briefed GAO officials on the plans for alignment and furnished them with a copy of the Secure Flight Concept of Operations and the Consolidated Users Guide. In addition, the upcoming Secure Flight Notice of Proposed Rule Making and Pre-Departure APIS Final Rule will outline the alignment plan in greater detail. Despite having been provided with this detailed update on this long-term program (as well as the Department's short-term solution), it does not appear this information was considered in the assessment.

***Performance Expectation 18***: *Deploy checkpoint technologies to address vulnerabilities*. The Department disagrees with the assessment of "Generally Not Achieved." This assessment does not recognize the Department's progress in this Performance Expectation, and does not consider the practical limitations inherent in developing and deploying new technological solutions.

Contrary to the statement in the GAO Report, the Department is constantly deploying existing technologies and developing new technologies to reduce checkpoint vulnerabilities. In particular, DHS-TSA continues to apply the latest improvements to existing technologies – such as checkpoint x-ray systems, walk-through metal detectors, and next-generation explosive trace detection systems. With regard to developing technologies, DHS-TSA is working closely with the DHS Science and Technology Directorate (DHS-S&T) on research and development activities to rapidly and responsibly respond to threats and to achieve advancements in screening technologies.

In Fiscal Year 2007, DHS-TSA and S&T explored technologies, such as bottled liquids scanners, whole body imagers, cast and prosthetics scanners, automated explosives detection devices, and advanced technology screening systems for carry-on items. The development of new technologies, however, takes time to test in the laboratory and in the field. Such testing must be conducted to determine operational effectiveness and suitability before new technologies can be deployed at operating checkpoints. The safety of the Nation and its citizens is too important to rush the deployment of untested technologies. Adequate testing before deployment also is needed to exercise proper stewardship of federal resources.

Furthermore, the GAO Report does not consider other efforts, in addition to checkpoint technologies, that have effectively reduced vulnerabilities. For example, DHS-TSA has instituted updated procedures to detect explosives and has provided enhanced training for Transportation Security Officers (TSO). Better educated and



trained TSOs are better equipped to recognize and deal with potentially threatening contraband. Deployment of TSOs specifically trained in behavioral recognition and bomb appraisal, as well as specially-trained canines, also enhances the safety of the current checkpoint screening procedures.

**Surface Transportation Security**

Although recognizing that the Department "Generally Achieved" three of the five performance expectations related to securing modes of surface transportation, the GAO Report does not recognize the progress that has been made by the Department in the remaining areas.

***Performance Expectation 3***: *Issue standards for securing surface transportation modes.* The GAO Report assessment of "Generally Not Achieved" is inaccurate and does not reflect the Department's significant progress. While recognizing the Department's issuance of standards related to mass transit and passenger and freight rail, the Report does not take into consideration standards issued by the Department in other modes of transportation, such as highways and pipelines.

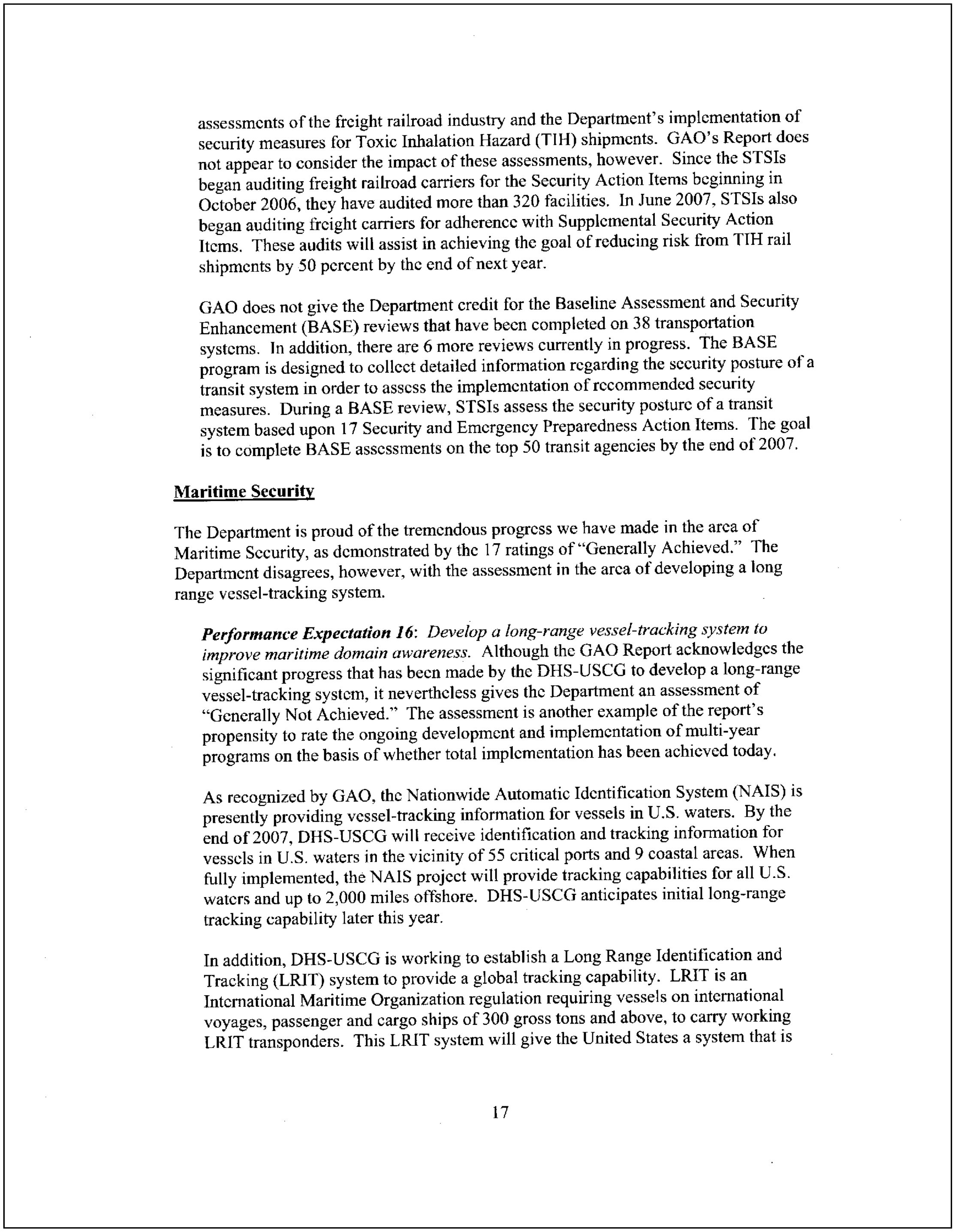
With respect to highways, DHS-TSA has developed draft Security Action Items (SAIs). Copies of the draft SAIs were provided to GAO officials in connection with a prior GAO audit on "Commercial Vehicle Security." These SAIs contained standards addressing personnel security, access control and *en route* security related to the highway modality.

With respect to pipelines, DHS-TSA issued "Pipeline Security Smart Practices" to pipeline industries in an effort to assist them in their security planning and implementation. These Smart Practices are drawn from the data collected from the numerous on-site security reviews of pipeline operators, personnel, and security measures conducted since the Fall of 2003. The Smart Practices contain voluntary standards that address badging and access control, physical security, vehicle checkpoint and intrusion detection, and security incident management planning. In addition, the Department of Transportation (DOT) issued the *Pipeline Security Information Circular* and the *Pipeline Security Contingency Planning Guidance* in 2002. DHS-TSA supports these standards, as they were used as the basis for its CSRs.

***Performance Expectation 4***: *Conduct compliance inspections for surface transportation systems.* The Department disagrees with the assessment of "Generally Not Achieved." Although the GAO Report recognizes that the Department has conducted compliance inspections with regard to the mass transit, passenger rail, and freight rail modes, its assessment does not appear to give DHS credit for these compliance inspections or the progress that has been made in other areas.

In particular, the GAO Report notes that DHS-TSA provided supplemental information regarding Surface Transportation Security Inspectors' (STSIs) on-site

16



assessments of the freight railroad industry and the Department's implementation of security measures for Toxic Inhalation Hazard (TIH) shipments. GAO's Report does not appear to consider the impact of these assessments, however. Since the STSIs began auditing freight railroad carriers for the Security Action Items beginning in October 2006, they have audited more than 320 facilities. In June 2007, STSIs also began auditing freight carriers for adherence with Supplemental Security Action Items. These audits will assist in achieving the goal of reducing risk from TIH rail shipments by 50 percent by the end of next year.

GAO does not give the Department credit for the Baseline Assessment and Security Enhancement (BASE) reviews that have been completed on 38 transportation systems. In addition, there are 6 more reviews currently in progress. The BASE program is designed to collect detailed information regarding the security posture of a transit system in order to assess the implementation of recommended security measures. During a BASE review, STSIs assess the security posture of a transit system based upon 17 Security and Emergency Preparedness Action Items. The goal is to complete BASE assessments on the top 50 transit agencies by the end of 2007.

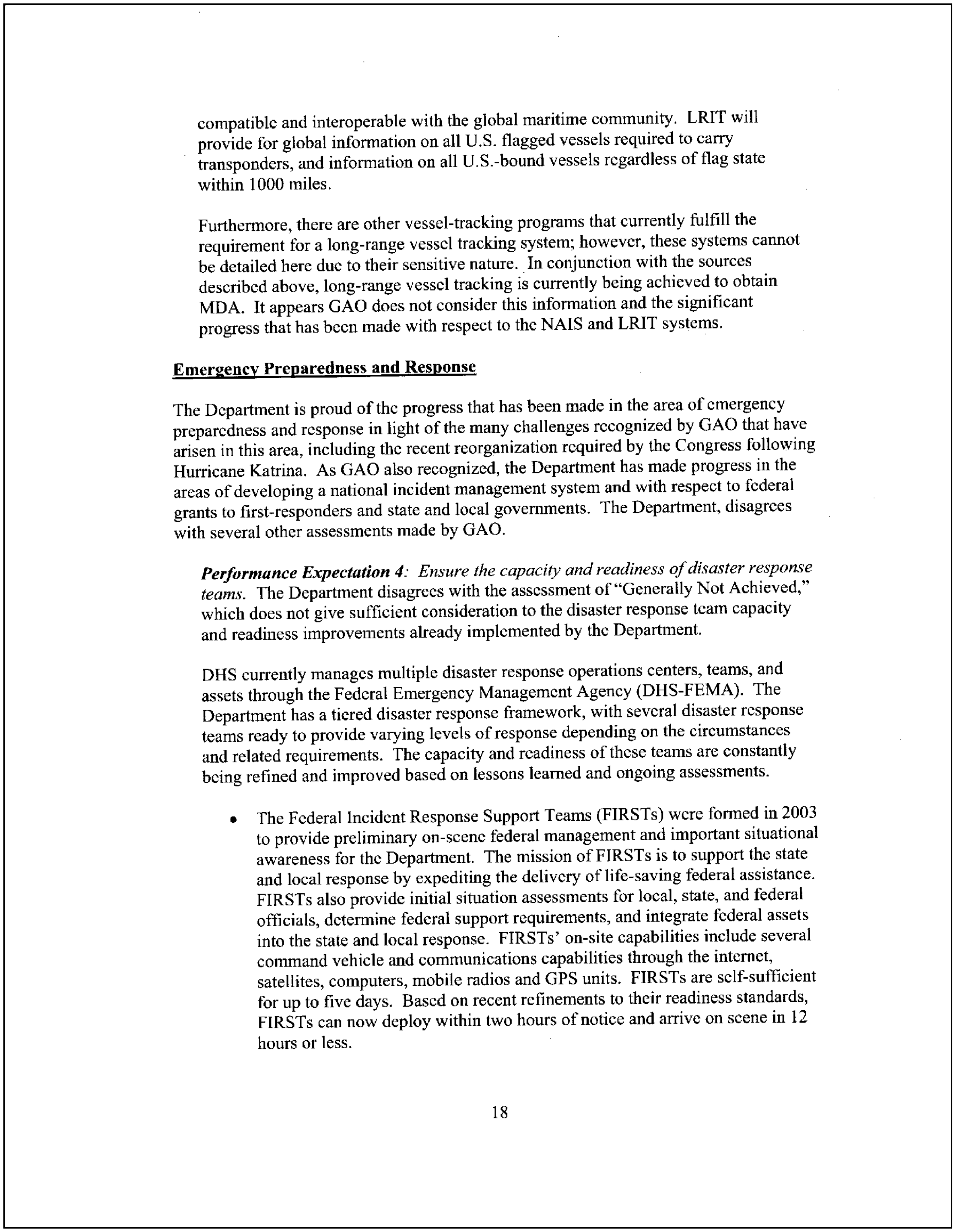
**Maritime Security**

The Department is proud of the tremendous progress we have made in the area of Maritime Security, as demonstrated by the 17 ratings of "Generally Achieved." The Department disagrees, however, with the assessment in the area of developing a long range vessel-tracking system.

***Performance Expectation 16**: Develop a long-range vessel-tracking system to improve maritime domain awareness.* Although the GAO Report acknowledges the significant progress that has been made by the DHS-USCG to develop a long-range vessel-tracking system, it nevertheless gives the Department an assessment of "Generally Not Achieved." The assessment is another example of the report's propensity to rate the ongoing development and implementation of multi-year programs on the basis of whether total implementation has been achieved today.

As recognized by GAO, the Nationwide Automatic Identification System (NAIS) is presently providing vessel-tracking information for vessels in U.S. waters. By the end of 2007, DHS-USCG will receive identification and tracking information for vessels in U.S. waters in the vicinity of 55 critical ports and 9 coastal areas. When fully implemented, the NAIS project will provide tracking capabilities for all U.S. waters and up to 2,000 miles offshore. DHS-USCG anticipates initial long-range tracking capability later this year.

In addition, DHS-USCG is working to establish a Long Range Identification and Tracking (LRIT) system to provide a global tracking capability. LRIT is an International Maritime Organization regulation requiring vessels on international voyages, passenger and cargo ships of 300 gross tons and above, to carry working LRIT transponders. This LRIT system will give the United States a system that is



compatible and interoperable with the global maritime community. LRIT will provide for global information on all U.S. flagged vessels required to carry transponders, and information on all U.S.-bound vessels regardless of flag state within 1000 miles.

Furthermore, there are other vessel-tracking programs that currently fulfill the requirement for a long-range vessel tracking system; however, these systems cannot be detailed here due to their sensitive nature. In conjunction with the sources described above, long-range vessel tracking is currently being achieved to obtain MDA. It appears GAO does not consider this information and the significant progress that has been made with respect to the NAIS and LRIT systems.

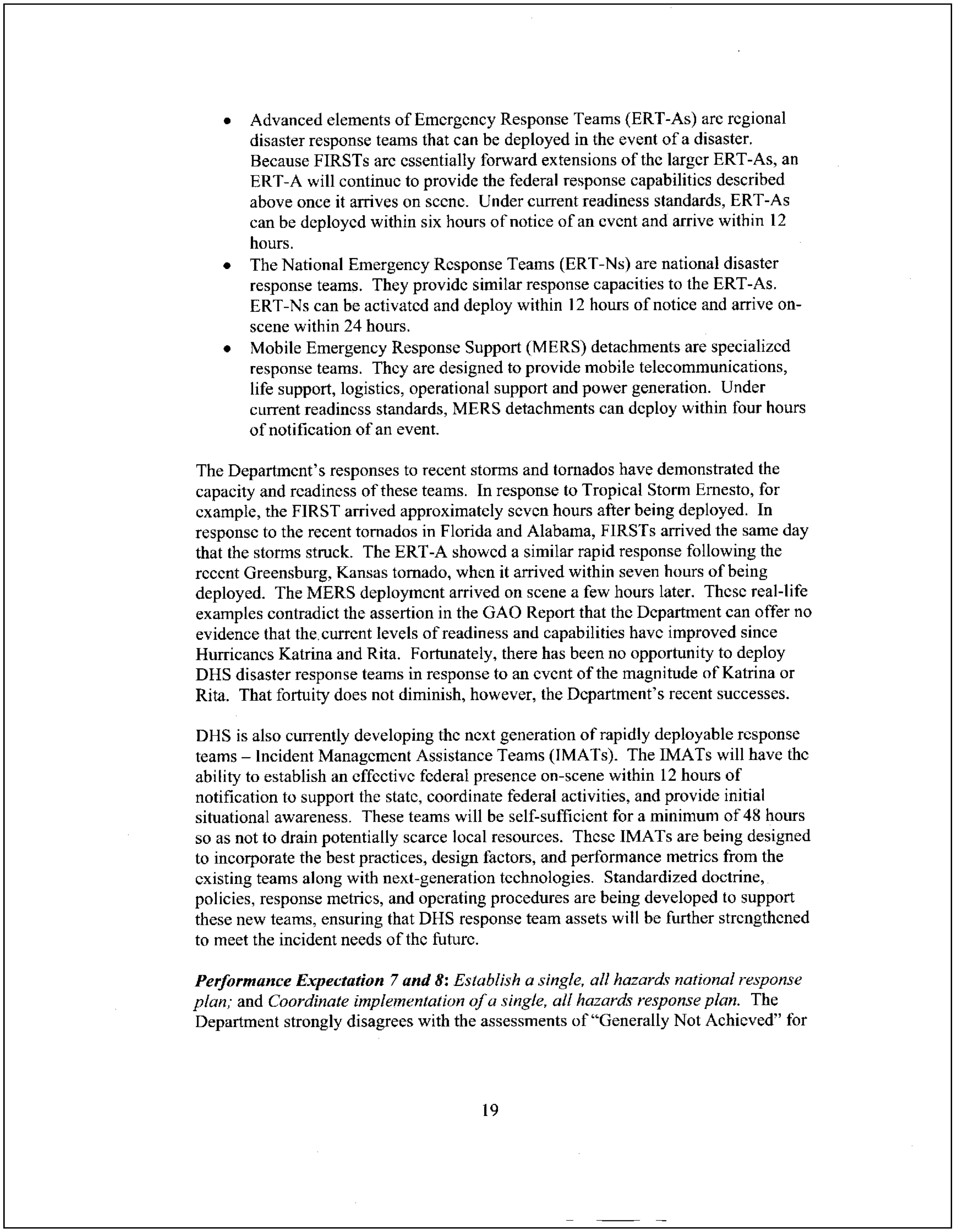
**Emergency Preparedness and Response**

The Department is proud of the progress that has been made in the area of emergency preparedness and response in light of the many challenges recognized by GAO that have arisen in this area, including the recent reorganization required by the Congress following Hurricane Katrina. As GAO also recognized, the Department has made progress in the areas of developing a national incident management system and with respect to federal grants to first-responders and state and local governments. The Department, disagrees with several other assessments made by GAO.

***Performance Expectation 4**: Ensure the capacity and readiness of disaster response teams.* The Department disagrees with the assessment of "Generally Not Achieved," which does not give sufficient consideration to the disaster response team capacity and readiness improvements already implemented by the Department.

DHS currently manages multiple disaster response operations centers, teams, and assets through the Federal Emergency Management Agency (DHS-FEMA). The Department has a tiered disaster response framework, with several disaster response teams ready to provide varying levels of response depending on the circumstances and related requirements. The capacity and readiness of these teams are constantly being refined and improved based on lessons learned and ongoing assessments.

- The Federal Incident Response Support Teams (FIRSTs) were formed in 2003 to provide preliminary on-scene federal management and important situational awareness for the Department. The mission of FIRSTs is to support the state and local response by expediting the delivery of life-saving federal assistance. FIRSTs also provide initial situation assessments for local, state, and federal officials, determine federal support requirements, and integrate federal assets into the state and local response. FIRSTs' on-site capabilities include several command vehicle and communications capabilities through the internet, satellites, computers, mobile radios and GPS units. FIRSTs are self-sufficient for up to five days. Based on recent refinements to their readiness standards, FIRSTs can now deploy within two hours of notice and arrive on scene in 12 hours or less.

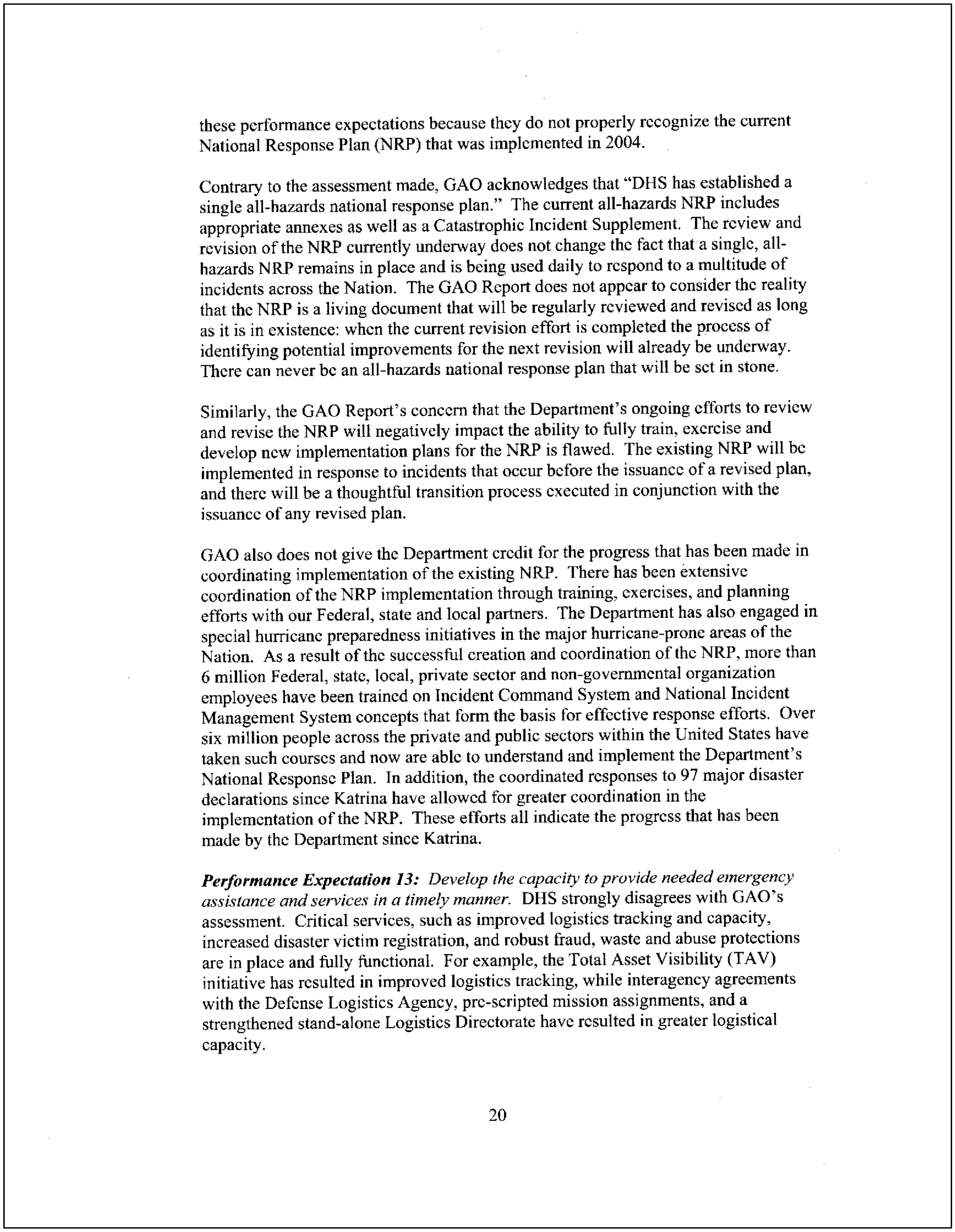


- Advanced elements of Emergency Response Teams (ERT-As) are regional disaster response teams that can be deployed in the event of a disaster. Because FIRSTs are essentially forward extensions of the larger ERT-As, an ERT-A will continue to provide the federal response capabilities described above once it arrives on scene. Under current readiness standards, ERT-As can be deployed within six hours of notice of an event and arrive within 12 hours.
- The National Emergency Response Teams (ERT-Ns) are national disaster response teams. They provide similar response capacities to the ERT-As. ERT-Ns can be activated and deploy within 12 hours of notice and arrive on-scene within 24 hours.
- Mobile Emergency Response Support (MERS) detachments are specialized response teams. They are designed to provide mobile telecommunications, life support, logistics, operational support and power generation. Under current readiness standards, MERS detachments can deploy within four hours of notification of an event.

The Department's responses to recent storms and tornados have demonstrated the capacity and readiness of these teams. In response to Tropical Storm Ernesto, for example, the FIRST arrived approximately seven hours after being deployed. In response to the recent tornados in Florida and Alabama, FIRSTs arrived the same day that the storms struck. The ERT-A showed a similar rapid response following the recent Greensburg, Kansas tornado, when it arrived within seven hours of being deployed. The MERS deployment arrived on scene a few hours later. These real-life examples contradict the assertion in the GAO Report that the Department can offer no evidence that the current levels of readiness and capabilities have improved since Hurricanes Katrina and Rita. Fortunately, there has been no opportunity to deploy DHS disaster response teams in response to an event of the magnitude of Katrina or Rita. That fortuity does not diminish, however, the Department's recent successes.

DHS is also currently developing the next generation of rapidly deployable response teams – Incident Management Assistance Teams (IMATs). The IMATs will have the ability to establish an effective federal presence on-scene within 12 hours of notification to support the state, coordinate federal activities, and provide initial situational awareness. These teams will be self-sufficient for a minimum of 48 hours so as not to drain potentially scarce local resources. These IMATs are being designed to incorporate the best practices, design factors, and performance metrics from the existing teams along with next-generation technologies. Standardized doctrine, policies, response metrics, and operating procedures are being developed to support these new teams, ensuring that DHS response team assets will be further strengthened to meet the incident needs of the future.

***Performance Expectation* 7 *and 8*:** *Establish a single, all hazards national response plan;* and *Coordinate implementation of a single, all hazards response plan.* The Department strongly disagrees with the assessments of "Generally Not Achieved" for



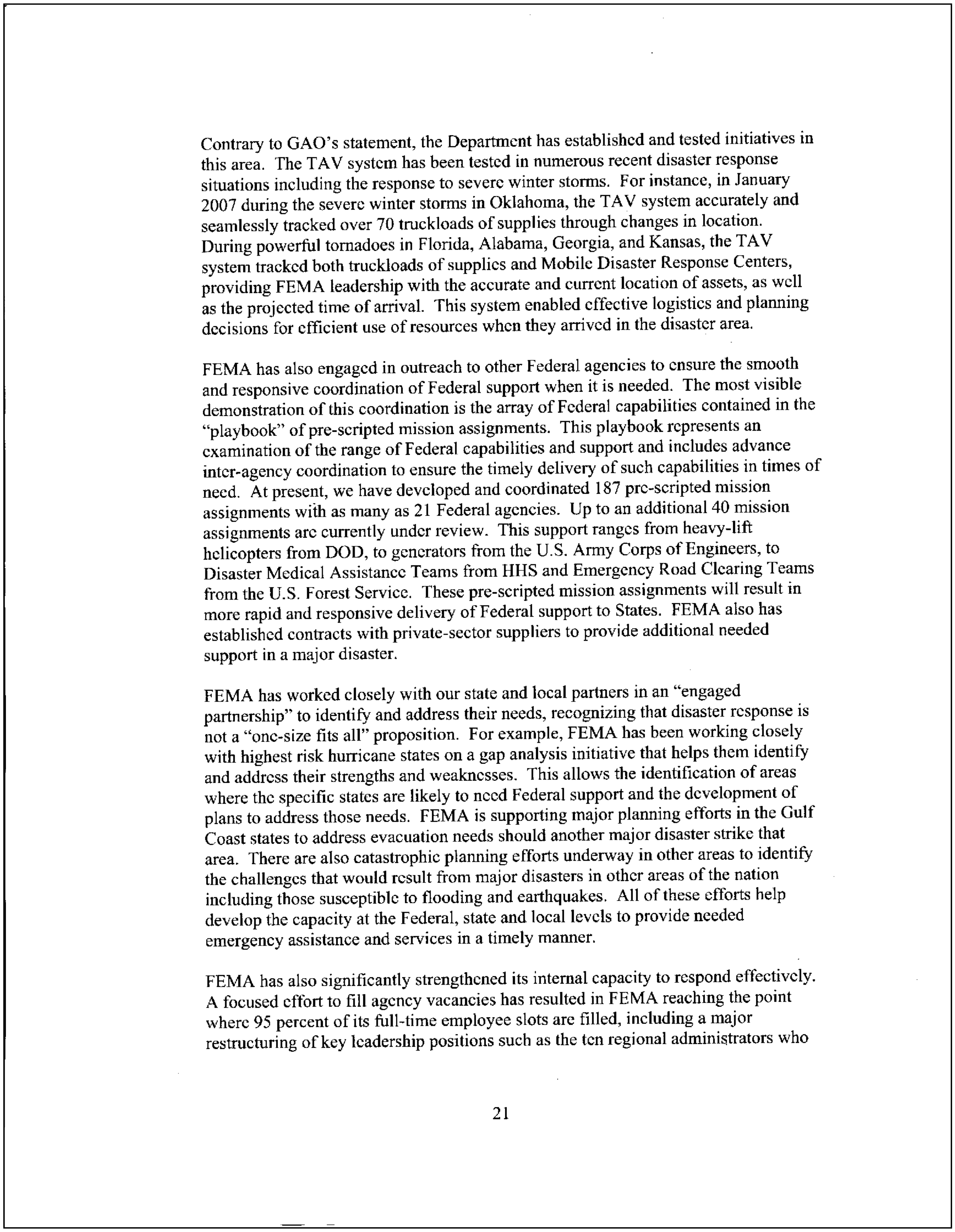
these performance expectations because they do not properly recognize the current National Response Plan (NRP) that was implemented in 2004.

Contrary to the assessment made, GAO acknowledges that "DHS has established a single all-hazards national response plan." The current all-hazards NRP includes appropriate annexes as well as a Catastrophic Incident Supplement. The review and revision of the NRP currently underway does not change the fact that a single, all-hazards NRP remains in place and is being used daily to respond to a multitude of incidents across the Nation. The GAO Report does not appear to consider the reality that the NRP is a living document that will be regularly reviewed and revised as long as it is in existence: when the current revision effort is completed the process of identifying potential improvements for the next revision will already be underway. There can never be an all-hazards national response plan that will be set in stone.

Similarly, the GAO Report's concern that the Department's ongoing efforts to review and revise the NRP will negatively impact the ability to fully train, exercise and develop new implementation plans for the NRP is flawed. The existing NRP will be implemented in response to incidents that occur before the issuance of a revised plan, and there will be a thoughtful transition process executed in conjunction with the issuance of any revised plan.

GAO also does not give the Department credit for the progress that has been made in coordinating implementation of the existing NRP. There has been extensive coordination of the NRP implementation through training, exercises, and planning efforts with our Federal, state and local partners. The Department has also engaged in special hurricane preparedness initiatives in the major hurricane-prone areas of the Nation. As a result of the successful creation and coordination of the NRP, more than 6 million Federal, state, local, private sector and non-governmental organization employees have been trained on Incident Command System and National Incident Management System concepts that form the basis for effective response efforts. Over six million people across the private and public sectors within the United States have taken such courses and now are able to understand and implement the Department's National Response Plan. In addition, the coordinated responses to 97 major disaster declarations since Katrina have allowed for greater coordination in the implementation of the NRP. These efforts all indicate the progress that has been made by the Department since Katrina.

***Performance Expectation 13:*** *Develop the capacity to provide needed emergency assistance and services in a timely manner.* DHS strongly disagrees with GAO's assessment. Critical services, such as improved logistics tracking and capacity, increased disaster victim registration, and robust fraud, waste and abuse protections are in place and fully functional. For example, the Total Asset Visibility (TAV) initiative has resulted in improved logistics tracking, while interagency agreements with the Defense Logistics Agency, pre-scripted mission assignments, and a strengthened stand-alone Logistics Directorate have resulted in greater logistical capacity.

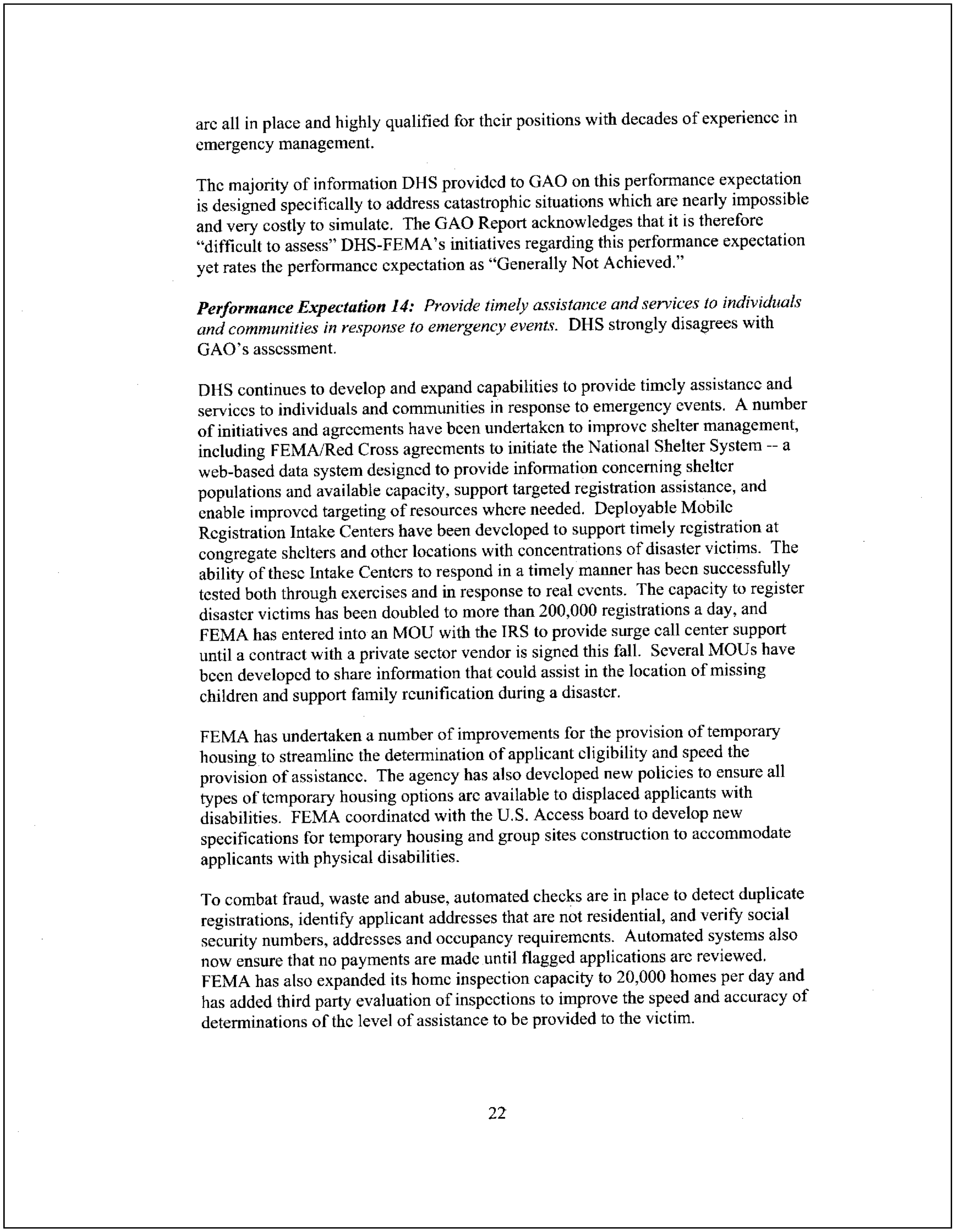


Contrary to GAO's statement, the Department has established and tested initiatives in this area. The TAV system has been tested in numerous recent disaster response situations including the response to severe winter storms. For instance, in January 2007 during the severe winter storms in Oklahoma, the TAV system accurately and seamlessly tracked over 70 truckloads of supplies through changes in location. During powerful tornadoes in Florida, Alabama, Georgia, and Kansas, the TAV system tracked both truckloads of supplies and Mobile Disaster Response Centers, providing FEMA leadership with the accurate and current location of assets, as well as the projected time of arrival. This system enabled effective logistics and planning decisions for efficient use of resources when they arrived in the disaster area.

FEMA has also engaged in outreach to other Federal agencies to ensure the smooth and responsive coordination of Federal support when it is needed. The most visible demonstration of this coordination is the array of Federal capabilities contained in the "playbook" of pre-scripted mission assignments. This playbook represents an examination of the range of Federal capabilities and support and includes advance inter-agency coordination to ensure the timely delivery of such capabilities in times of need. At present, we have developed and coordinated 187 pre-scripted mission assignments with as many as 21 Federal agencies. Up to an additional 40 mission assignments are currently under review. This support ranges from heavy-lift helicopters from DOD, to generators from the U.S. Army Corps of Engineers, to Disaster Medical Assistance Teams from HHS and Emergency Road Clearing Teams from the U.S. Forest Service. These pre-scripted mission assignments will result in more rapid and responsive delivery of Federal support to States. FEMA also has established contracts with private-sector suppliers to provide additional needed support in a major disaster.

FEMA has worked closely with our state and local partners in an "engaged partnership" to identify and address their needs, recognizing that disaster response is not a "one-size fits all" proposition. For example, FEMA has been working closely with highest risk hurricane states on a gap analysis initiative that helps them identify and address their strengths and weaknesses. This allows the identification of areas where the specific states are likely to need Federal support and the development of plans to address those needs. FEMA is supporting major planning efforts in the Gulf Coast states to address evacuation needs should another major disaster strike that area. There are also catastrophic planning efforts underway in other areas to identify the challenges that would result from major disasters in other areas of the nation including those susceptible to flooding and earthquakes. All of these efforts help develop the capacity at the Federal, state and local levels to provide needed emergency assistance and services in a timely manner.

FEMA has also significantly strengthened its internal capacity to respond effectively. A focused effort to fill agency vacancies has resulted in FEMA reaching the point where 95 percent of its full-time employee slots are filled, including a major restructuring of key leadership positions such as the ten regional administrators who



are all in place and highly qualified for their positions with decades of experience in emergency management.

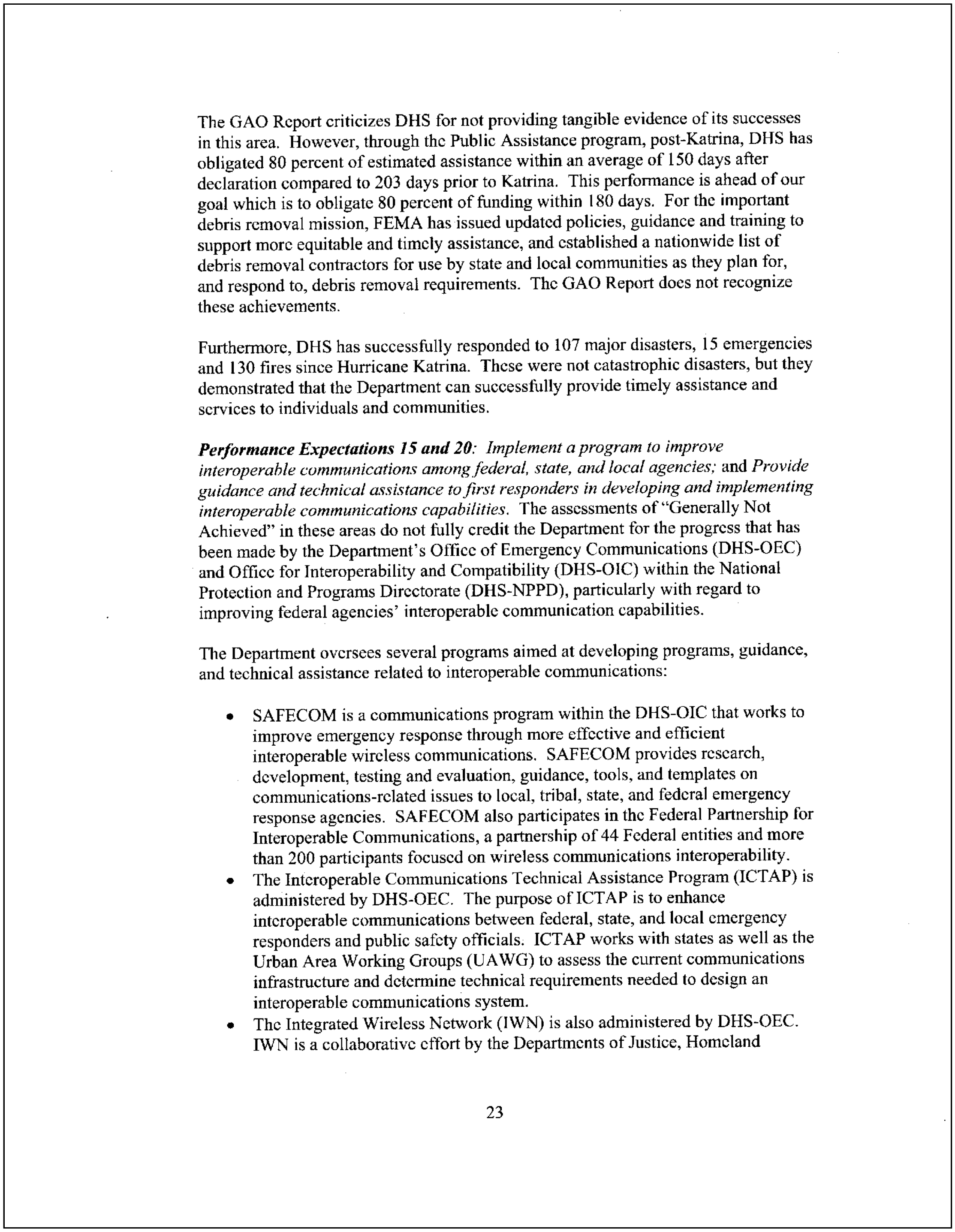
The majority of information DHS provided to GAO on this performance expectation is designed specifically to address catastrophic situations which are nearly impossible and very costly to simulate. The GAO Report acknowledges that it is therefore "difficult to assess" DHS-FEMA's initiatives regarding this performance expectation yet rates the performance expectation as "Generally Not Achieved."

***Performance Expectation 14:*** *Provide timely assistance and services to individuals and communities in response to emergency events.* DHS strongly disagrees with GAO's assessment.

DHS continues to develop and expand capabilities to provide timely assistance and services to individuals and communities in response to emergency events. A number of initiatives and agreements have been undertaken to improve shelter management, including FEMA/Red Cross agreements to initiate the National Shelter System -- a web-based data system designed to provide information concerning shelter populations and available capacity, support targeted registration assistance, and enable improved targeting of resources where needed. Deployable Mobile Registration Intake Centers have been developed to support timely registration at congregate shelters and other locations with concentrations of disaster victims. The ability of these Intake Centers to respond in a timely manner has been successfully tested both through exercises and in response to real events. The capacity to register disaster victims has been doubled to more than 200,000 registrations a day, and FEMA has entered into an MOU with the IRS to provide surge call center support until a contract with a private sector vendor is signed this fall. Several MOUs have been developed to share information that could assist in the location of missing children and support family reunification during a disaster.

FEMA has undertaken a number of improvements for the provision of temporary housing to streamline the determination of applicant eligibility and speed the provision of assistance. The agency has also developed new policies to ensure all types of temporary housing options are available to displaced applicants with disabilities. FEMA coordinated with the U.S. Access board to develop new specifications for temporary housing and group sites construction to accommodate applicants with physical disabilities.

To combat fraud, waste and abuse, automated checks are in place to detect duplicate registrations, identify applicant addresses that are not residential, and verify social security numbers, addresses and occupancy requirements. Automated systems also now ensure that no payments are made until flagged applications are reviewed. FEMA has also expanded its home inspection capacity to 20,000 homes per day and has added third party evaluation of inspections to improve the speed and accuracy of determinations of the level of assistance to be provided to the victim.



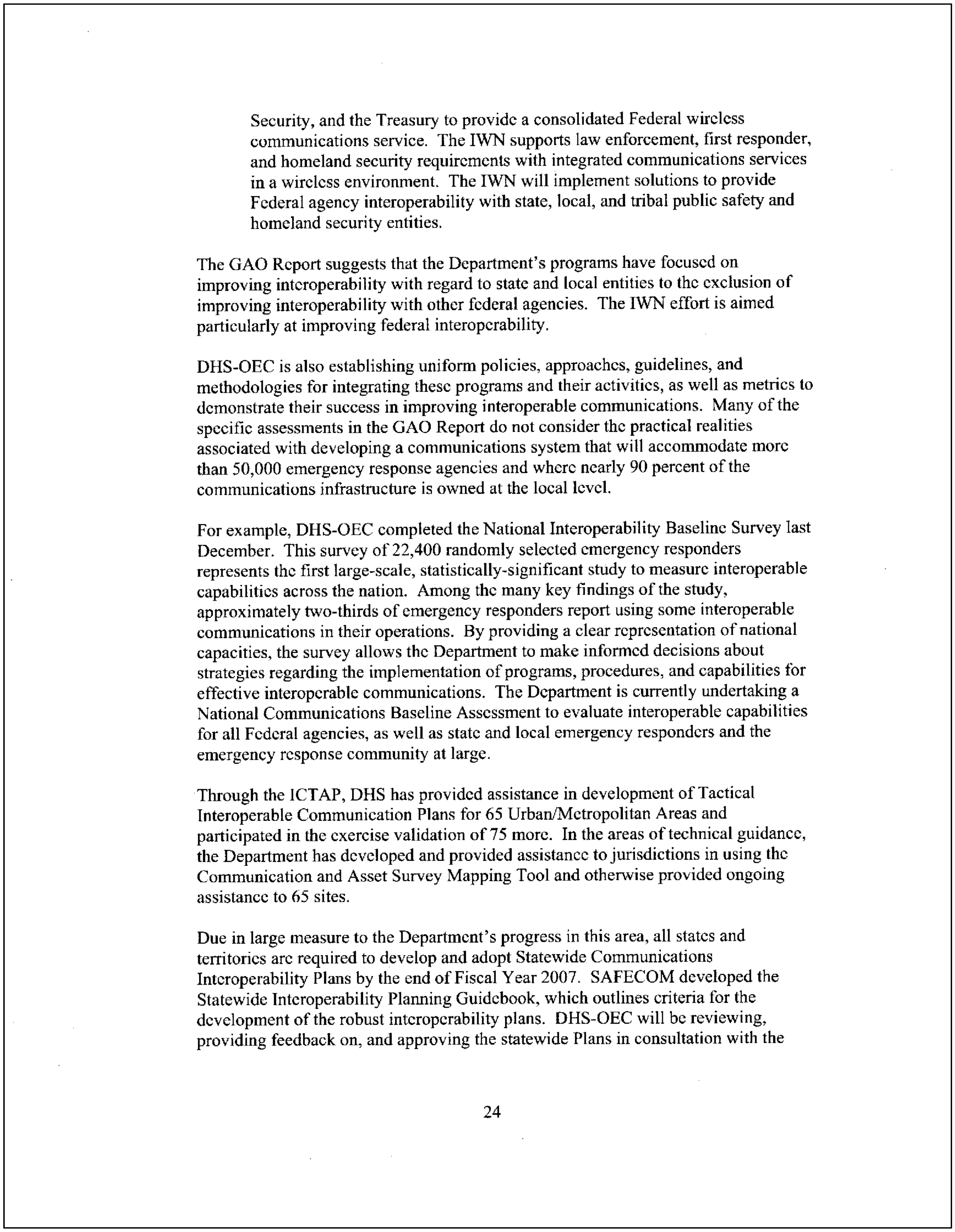
The GAO Report criticizes DHS for not providing tangible evidence of its successes in this area. However, through the Public Assistance program, post-Katrina, DHS has obligated 80 percent of estimated assistance within an average of 150 days after declaration compared to 203 days prior to Katrina. This performance is ahead of our goal which is to obligate 80 percent of funding within 180 days. For the important debris removal mission, FEMA has issued updated policies, guidance and training to support more equitable and timely assistance, and established a nationwide list of debris removal contractors for use by state and local communities as they plan for, and respond to, debris removal requirements. The GAO Report does not recognize these achievements.

Furthermore, DHS has successfully responded to 107 major disasters, 15 emergencies and 130 fires since Hurricane Katrina. These were not catastrophic disasters, but they demonstrated that the Department can successfully provide timely assistance and services to individuals and communities.

***Performance Expectations 15 and 20****: Implement a program to improve interoperable communications among federal, state, and local agencies;* and *Provide guidance and technical assistance to first responders in developing and implementing interoperable communications capabilities.* The assessments of "Generally Not Achieved" in these areas do not fully credit the Department for the progress that has been made by the Department's Office of Emergency Communications (DHS-OEC) and Office for Interoperability and Compatibility (DHS-OIC) within the National Protection and Programs Directorate (DHS-NPPD), particularly with regard to improving federal agencies' interoperable communication capabilities.

The Department oversees several programs aimed at developing programs, guidance, and technical assistance related to interoperable communications:

- SAFECOM is a communications program within the DHS-OIC that works to improve emergency response through more effective and efficient interoperable wireless communications. SAFECOM provides research, development, testing and evaluation, guidance, tools, and templates on communications-related issues to local, tribal, state, and federal emergency response agencies. SAFECOM also participates in the Federal Partnership for Interoperable Communications, a partnership of 44 Federal entities and more than 200 participants focused on wireless communications interoperability.
- The Interoperable Communications Technical Assistance Program (ICTAP) is administered by DHS-OEC. The purpose of ICTAP is to enhance interoperable communications between federal, state, and local emergency responders and public safety officials. ICTAP works with states as well as the Urban Area Working Groups (UAWG) to assess the current communications infrastructure and determine technical requirements needed to design an interoperable communications system.
- The Integrated Wireless Network (IWN) is also administered by DHS-OEC. IWN is a collaborative effort by the Departments of Justice, Homeland



> Security, and the Treasury to provide a consolidated Federal wireless communications service. The IWN supports law enforcement, first responder, and homeland security requirements with integrated communications services in a wireless environment. The IWN will implement solutions to provide Federal agency interoperability with state, local, and tribal public safety and homeland security entities.

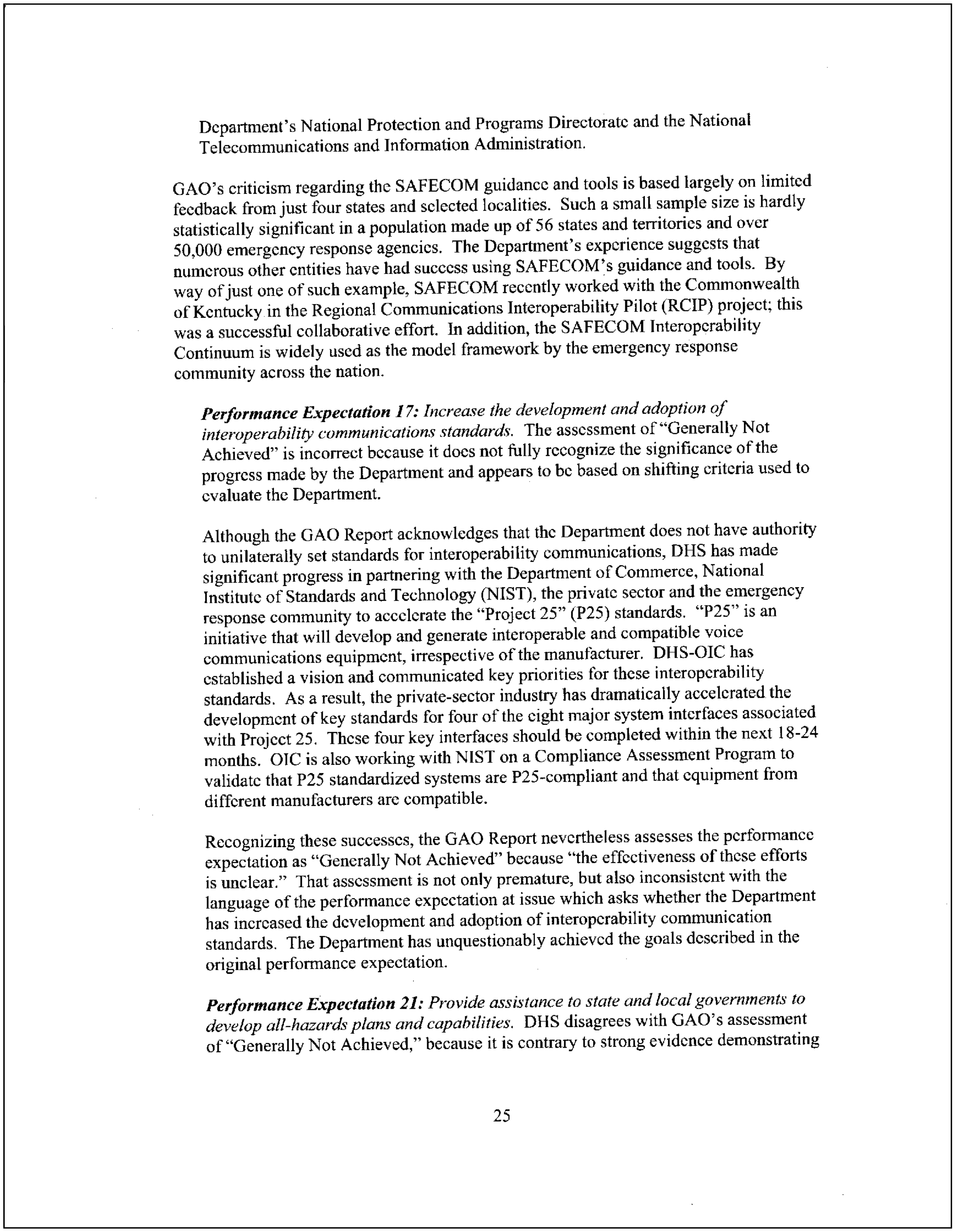
The GAO Report suggests that the Department's programs have focused on improving interoperability with regard to state and local entities to the exclusion of improving interoperability with other federal agencies. The IWN effort is aimed particularly at improving federal interoperability.

DHS-OEC is also establishing uniform policies, approaches, guidelines, and methodologies for integrating these programs and their activities, as well as metrics to demonstrate their success in improving interoperable communications. Many of the specific assessments in the GAO Report do not consider the practical realities associated with developing a communications system that will accommodate more than 50,000 emergency response agencies and where nearly 90 percent of the communications infrastructure is owned at the local level.

For example, DHS-OEC completed the National Interoperability Baseline Survey last December. This survey of 22,400 randomly selected emergency responders represents the first large-scale, statistically-significant study to measure interoperable capabilities across the nation. Among the many key findings of the study, approximately two-thirds of emergency responders report using some interoperable communications in their operations. By providing a clear representation of national capacities, the survey allows the Department to make informed decisions about strategies regarding the implementation of programs, procedures, and capabilities for effective interoperable communications. The Department is currently undertaking a National Communications Baseline Assessment to evaluate interoperable capabilities for all Federal agencies, as well as state and local emergency responders and the emergency response community at large.

Through the ICTAP, DHS has provided assistance in development of Tactical Interoperable Communication Plans for 65 Urban/Metropolitan Areas and participated in the exercise validation of 75 more. In the areas of technical guidance, the Department has developed and provided assistance to jurisdictions in using the Communication and Asset Survey Mapping Tool and otherwise provided ongoing assistance to 65 sites.

Due in large measure to the Department's progress in this area, all states and territories are required to develop and adopt Statewide Communications Interoperability Plans by the end of Fiscal Year 2007. SAFECOM developed the Statewide Interoperability Planning Guidebook, which outlines criteria for the development of the robust interoperability plans. DHS-OEC will be reviewing, providing feedback on, and approving the statewide Plans in consultation with the



Department's National Protection and Programs Directorate and the National Telecommunications and Information Administration.

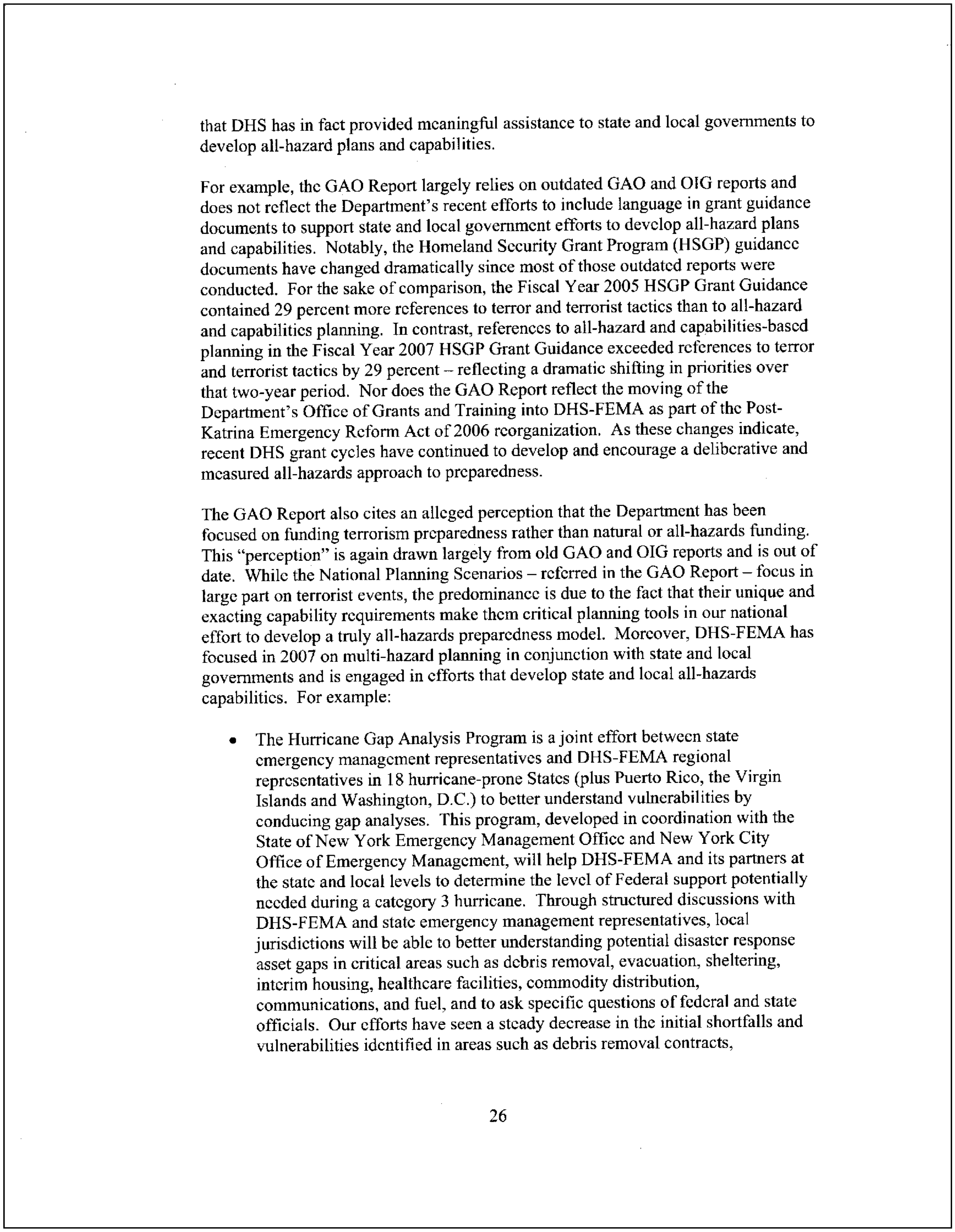
GAO's criticism regarding the SAFECOM guidance and tools is based largely on limited feedback from just four states and selected localities. Such a small sample size is hardly statistically significant in a population made up of 56 states and territories and over 50,000 emergency response agencies. The Department's experience suggests that numerous other entities have had success using SAFECOM's guidance and tools. By way of just one of such example, SAFECOM recently worked with the Commonwealth of Kentucky in the Regional Communications Interoperability Pilot (RCIP) project; this was a successful collaborative effort. In addition, the SAFECOM Interoperability Continuum is widely used as the model framework by the emergency response community across the nation.

***Performance Expectation 17:*** *Increase the development and adoption of interoperability communications standards.* The assessment of "Generally Not Achieved" is incorrect because it does not fully recognize the significance of the progress made by the Department and appears to be based on shifting criteria used to evaluate the Department.

Although the GAO Report acknowledges that the Department does not have authority to unilaterally set standards for interoperability communications, DHS has made significant progress in partnering with the Department of Commerce, National Institute of Standards and Technology (NIST), the private sector and the emergency response community to accelerate the "Project 25" (P25) standards. "P25" is an initiative that will develop and generate interoperable and compatible voice communications equipment, irrespective of the manufacturer. DHS-OIC has established a vision and communicated key priorities for these interoperability standards. As a result, the private-sector industry has dramatically accelerated the development of key standards for four of the eight major system interfaces associated with Project 25. These four key interfaces should be completed within the next 18-24 months. OIC is also working with NIST on a Compliance Assessment Program to validate that P25 standardized systems are P25-compliant and that equipment from different manufacturers are compatible.

Recognizing these successes, the GAO Report nevertheless assesses the performance expectation as "Generally Not Achieved" because "the effectiveness of these efforts is unclear." That assessment is not only premature, but also inconsistent with the language of the performance expectation at issue which asks whether the Department has increased the development and adoption of interoperability communication standards. The Department has unquestionably achieved the goals described in the original performance expectation.

***Performance Expectation 21:*** *Provide assistance to state and local governments to develop all-hazards plans and capabilities.* DHS disagrees with GAO's assessment of "Generally Not Achieved," because it is contrary to strong evidence demonstrating

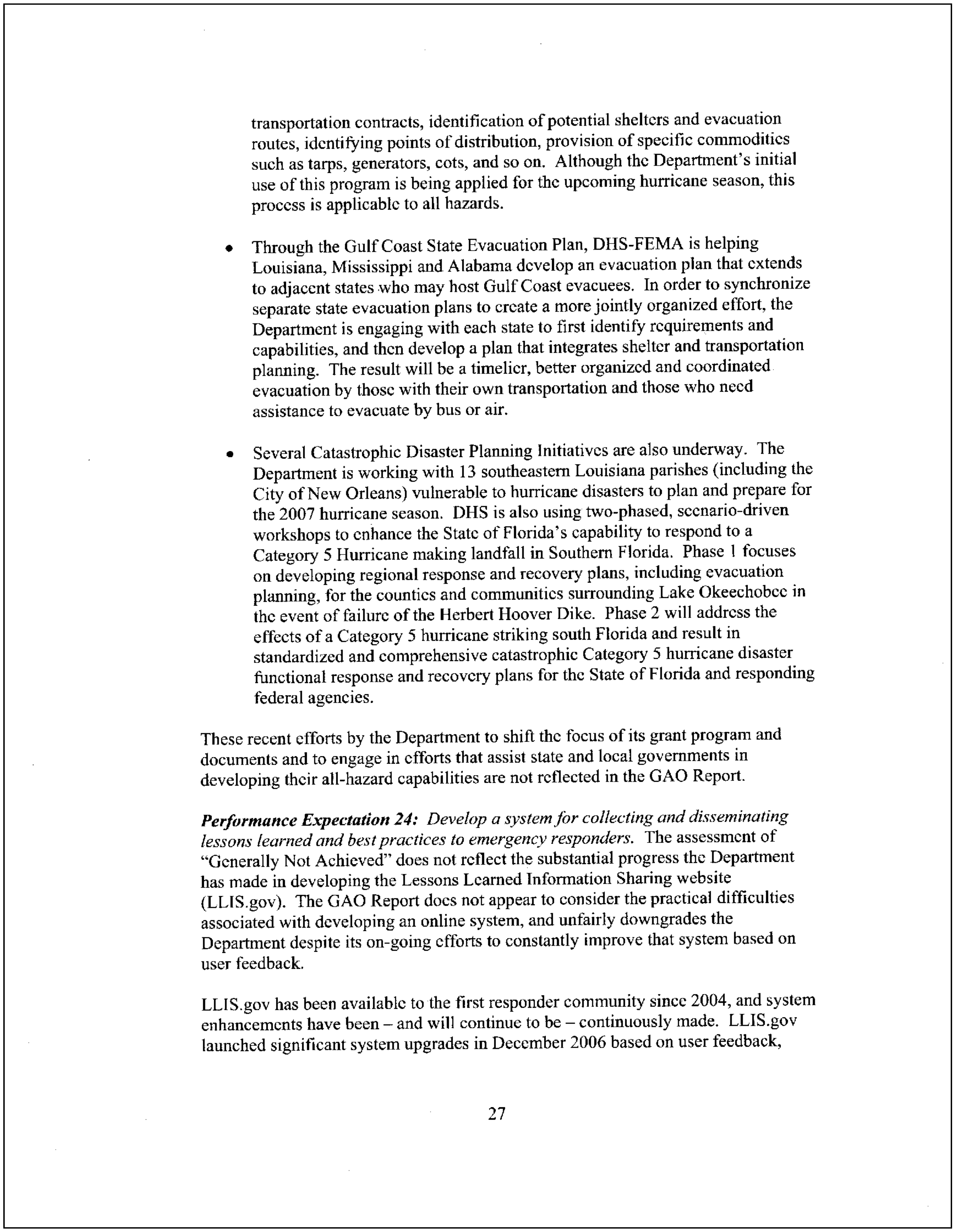


that DHS has in fact provided meaningful assistance to state and local governments to develop all-hazard plans and capabilities.

For example, the GAO Report largely relies on outdated GAO and OIG reports and does not reflect the Department's recent efforts to include language in grant guidance documents to support state and local government efforts to develop all-hazard plans and capabilities. Notably, the Homeland Security Grant Program (HSGP) guidance documents have changed dramatically since most of those outdated reports were conducted. For the sake of comparison, the Fiscal Year 2005 HSGP Grant Guidance contained 29 percent more references to terror and terrorist tactics than to all-hazard and capabilities planning. In contrast, references to all-hazard and capabilities-based planning in the Fiscal Year 2007 HSGP Grant Guidance exceeded references to terror and terrorist tactics by 29 percent – reflecting a dramatic shifting in priorities over that two-year period. Nor does the GAO Report reflect the moving of the Department's Office of Grants and Training into DHS-FEMA as part of the Post-Katrina Emergency Reform Act of 2006 reorganization. As these changes indicate, recent DHS grant cycles have continued to develop and encourage a deliberative and measured all-hazards approach to preparedness.

The GAO Report also cites an alleged perception that the Department has been focused on funding terrorism preparedness rather than natural or all-hazards funding. This "perception" is again drawn largely from old GAO and OIG reports and is out of date. While the National Planning Scenarios – referred in the GAO Report – focus in large part on terrorist events, the predominance is due to the fact that their unique and exacting capability requirements make them critical planning tools in our national effort to develop a truly all-hazards preparedness model. Moreover, DHS-FEMA has focused in 2007 on multi-hazard planning in conjunction with state and local governments and is engaged in efforts that develop state and local all-hazards capabilities. For example:

- The Hurricane Gap Analysis Program is a joint effort between state emergency management representatives and DHS-FEMA regional representatives in 18 hurricane-prone States (plus Puerto Rico, the Virgin Islands and Washington, D.C.) to better understand vulnerabilities by conducing gap analyses. This program, developed in coordination with the State of New York Emergency Management Office and New York City Office of Emergency Management, will help DHS-FEMA and its partners at the state and local levels to determine the level of Federal support potentially needed during a category 3 hurricane. Through structured discussions with DHS-FEMA and state emergency management representatives, local jurisdictions will be able to better understanding potential disaster response asset gaps in critical areas such as debris removal, evacuation, sheltering, interim housing, healthcare facilities, commodity distribution, communications, and fuel, and to ask specific questions of federal and state officials. Our efforts have seen a steady decrease in the initial shortfalls and vulnerabilities identified in areas such as debris removal contracts,



transportation contracts, identification of potential shelters and evacuation routes, identifying points of distribution, provision of specific commodities such as tarps, generators, cots, and so on. Although the Department's initial use of this program is being applied for the upcoming hurricane season, this process is applicable to all hazards.

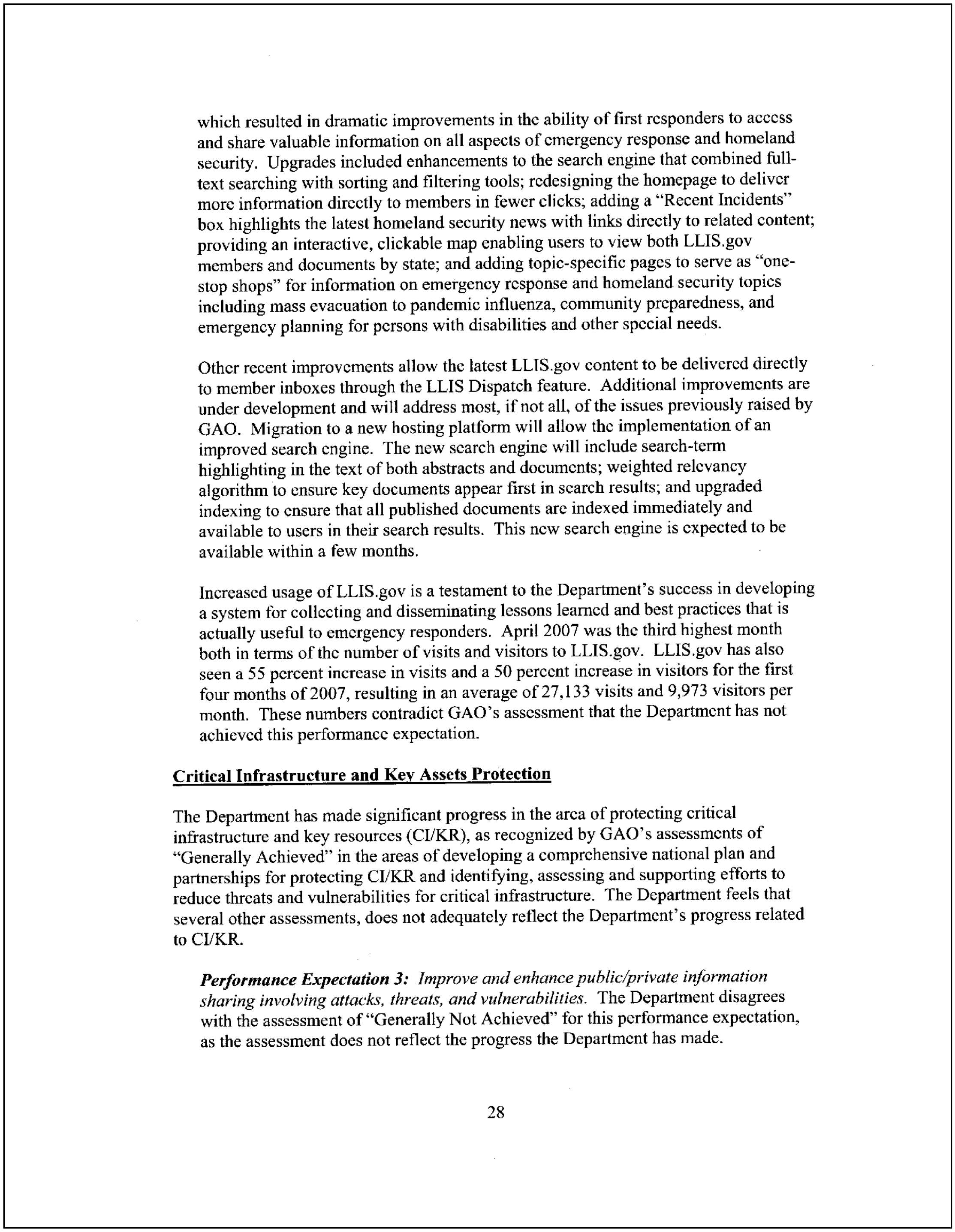
- Through the Gulf Coast State Evacuation Plan, DHS-FEMA is helping Louisiana, Mississippi and Alabama develop an evacuation plan that extends to adjacent states who may host Gulf Coast evacuees. In order to synchronize separate state evacuation plans to create a more jointly organized effort, the Department is engaging with each state to first identify requirements and capabilities, and then develop a plan that integrates shelter and transportation planning. The result will be a timelier, better organized and coordinated evacuation by those with their own transportation and those who need assistance to evacuate by bus or air.

- Several Catastrophic Disaster Planning Initiatives are also underway. The Department is working with 13 southeastern Louisiana parishes (including the City of New Orleans) vulnerable to hurricane disasters to plan and prepare for the 2007 hurricane season. DHS is also using two-phased, scenario-driven workshops to enhance the State of Florida's capability to respond to a Category 5 Hurricane making landfall in Southern Florida. Phase 1 focuses on developing regional response and recovery plans, including evacuation planning, for the counties and communities surrounding Lake Okeechobee in the event of failure of the Herbert Hoover Dike. Phase 2 will address the effects of a Category 5 hurricane striking south Florida and result in standardized and comprehensive catastrophic Category 5 hurricane disaster functional response and recovery plans for the State of Florida and responding federal agencies.

These recent efforts by the Department to shift the focus of its grant program and documents and to engage in efforts that assist state and local governments in developing their all-hazard capabilities are not reflected in the GAO Report.

***Performance Expectation 24:*** *Develop a system for collecting and disseminating lessons learned and best practices to emergency responders.* The assessment of "Generally Not Achieved" does not reflect the substantial progress the Department has made in developing the Lessons Learned Information Sharing website (LLIS.gov). The GAO Report does not appear to consider the practical difficulties associated with developing an online system, and unfairly downgrades the Department despite its on-going efforts to constantly improve that system based on user feedback.

LLIS.gov has been available to the first responder community since 2004, and system enhancements have been – and will continue to be – continuously made. LLIS.gov launched significant system upgrades in December 2006 based on user feedback,



which resulted in dramatic improvements in the ability of first responders to access and share valuable information on all aspects of emergency response and homeland security. Upgrades included enhancements to the search engine that combined full-text searching with sorting and filtering tools; redesigning the homepage to deliver more information directly to members in fewer clicks; adding a “Recent Incidents” box highlights the latest homeland security news with links directly to related content; providing an interactive, clickable map enabling users to view both LLIS.gov members and documents by state; and adding topic-specific pages to serve as “one-stop shops” for information on emergency response and homeland security topics including mass evacuation to pandemic influenza, community preparedness, and emergency planning for persons with disabilities and other special needs.

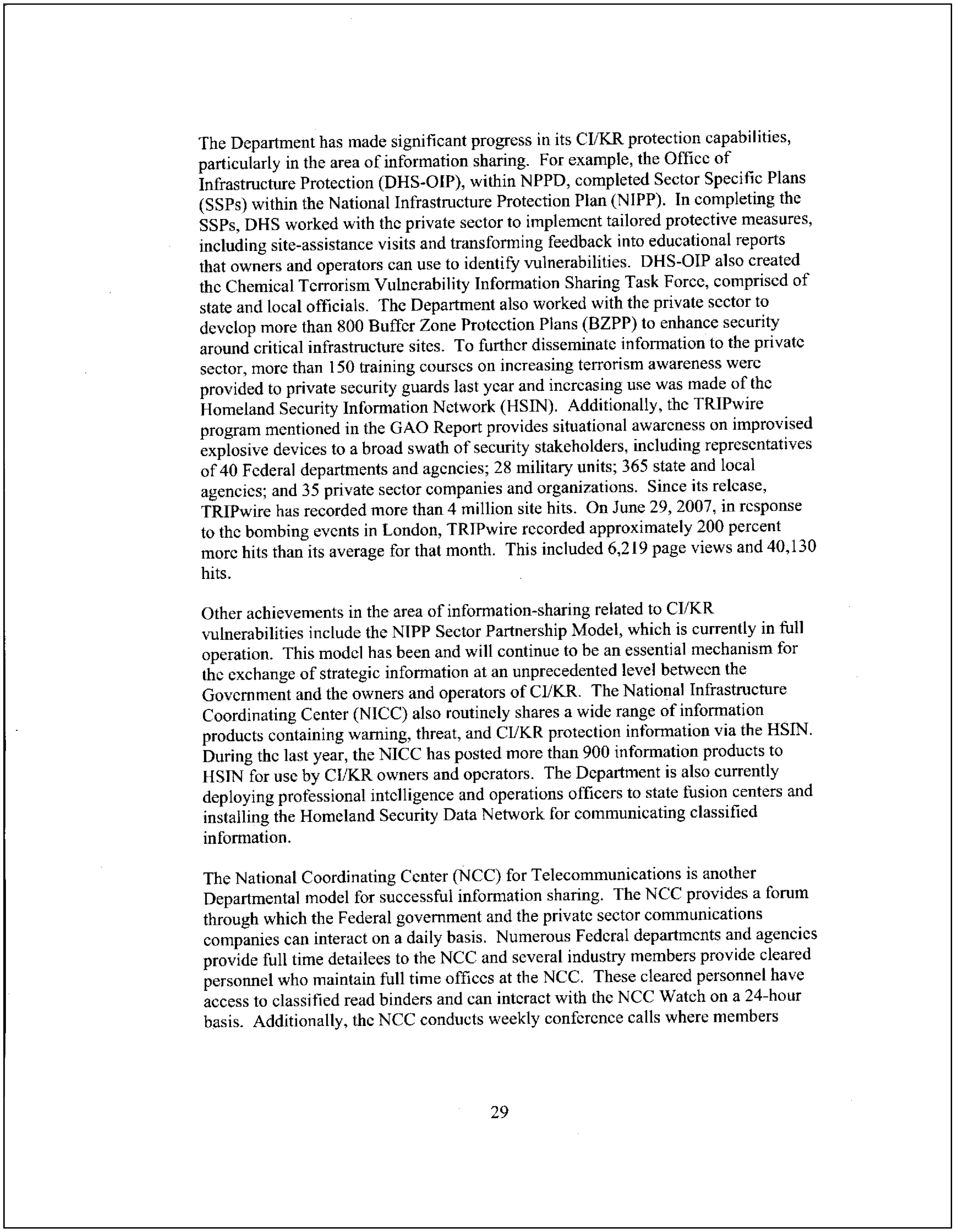
Other recent improvements allow the latest LLIS.gov content to be delivered directly to member inboxes through the LLIS Dispatch feature. Additional improvements are under development and will address most, if not all, of the issues previously raised by GAO. Migration to a new hosting platform will allow the implementation of an improved search engine. The new search engine will include search-term highlighting in the text of both abstracts and documents; weighted relevancy algorithm to ensure key documents appear first in search results; and upgraded indexing to ensure that all published documents are indexed immediately and available to users in their search results. This new search engine is expected to be available within a few months.

Increased usage of LLIS.gov is a testament to the Department’s success in developing a system for collecting and disseminating lessons learned and best practices that is actually useful to emergency responders. April 2007 was the third highest month both in terms of the number of visits and visitors to LLIS.gov. LLIS.gov has also seen a 55 percent increase in visits and a 50 percent increase in visitors for the first four months of 2007, resulting in an average of 27,133 visits and 9,973 visitors per month. These numbers contradict GAO’s assessment that the Department has not achieved this performance expectation.

## Critical Infrastructure and Key Assets Protection

The Department has made significant progress in the area of protecting critical infrastructure and key resources (CI/KR), as recognized by GAO’s assessments of “Generally Achieved” in the areas of developing a comprehensive national plan and partnerships for protecting CI/KR and identifying, assessing and supporting efforts to reduce threats and vulnerabilities for critical infrastructure. The Department feels that several other assessments, does not adequately reflect the Department’s progress related to CI/KR.

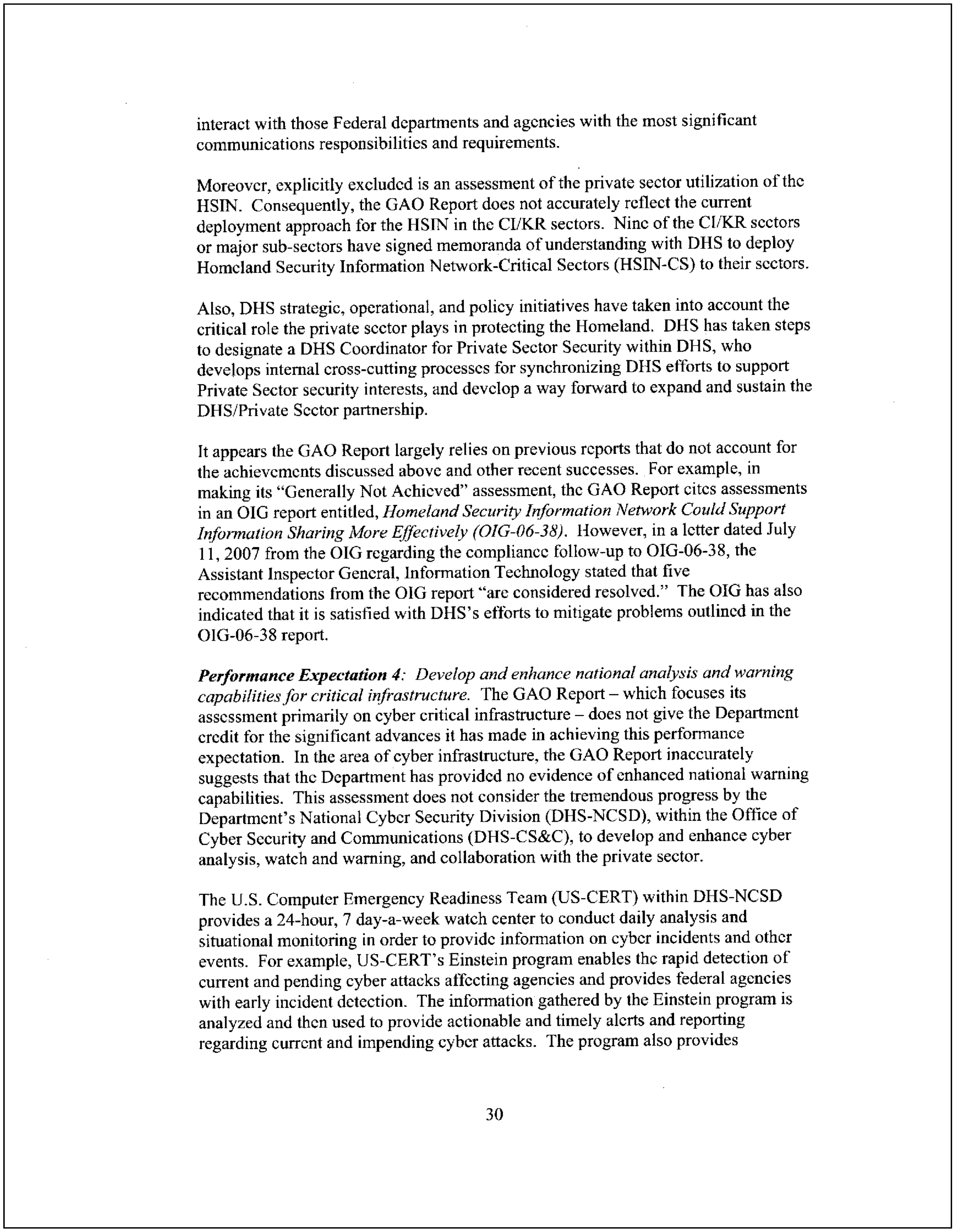
***Performance Expectation 3:*** *Improve and enhance public/private information sharing involving attacks, threats, and vulnerabilities.* The Department disagrees with the assessment of “Generally Not Achieved” for this performance expectation, as the assessment does not reflect the progress the Department has made.



The Department has made significant progress in its CI/KR protection capabilities, particularly in the area of information sharing. For example, the Office of Infrastructure Protection (DHS-OIP), within NPPD, completed Sector Specific Plans (SSPs) within the National Infrastructure Protection Plan (NIPP). In completing the SSPs, DHS worked with the private sector to implement tailored protective measures, including site-assistance visits and transforming feedback into educational reports that owners and operators can use to identify vulnerabilities. DHS-OIP also created the Chemical Terrorism Vulnerability Information Sharing Task Force, comprised of state and local officials. The Department also worked with the private sector to develop more than 800 Buffer Zone Protection Plans (BZPP) to enhance security around critical infrastructure sites. To further disseminate information to the private sector, more than 150 training courses on increasing terrorism awareness were provided to private security guards last year and increasing use was made of the Homeland Security Information Network (HSIN). Additionally, the TRIPwire program mentioned in the GAO Report provides situational awareness on improvised explosive devices to a broad swath of security stakeholders, including representatives of 40 Federal departments and agencies; 28 military units; 365 state and local agencies; and 35 private sector companies and organizations. Since its release, TRIPwire has recorded more than 4 million site hits. On June 29, 2007, in response to the bombing events in London, TRIPwire recorded approximately 200 percent more hits than its average for that month. This included 6,219 page views and 40,130 hits.

Other achievements in the area of information-sharing related to CI/KR vulnerabilities include the NIPP Sector Partnership Model, which is currently in full operation. This model has been and will continue to be an essential mechanism for the exchange of strategic information at an unprecedented level between the Government and the owners and operators of CI/KR. The National Infrastructure Coordinating Center (NICC) also routinely shares a wide range of information products containing warning, threat, and CI/KR protection information via the HSIN. During the last year, the NICC has posted more than 900 information products to HSIN for use by CI/KR owners and operators. The Department is also currently deploying professional intelligence and operations officers to state fusion centers and installing the Homeland Security Data Network for communicating classified information.

The National Coordinating Center (NCC) for Telecommunications is another Departmental model for successful information sharing. The NCC provides a forum through which the Federal government and the private sector communications companies can interact on a daily basis. Numerous Federal departments and agencies provide full time detailees to the NCC and several industry members provide cleared personnel who maintain full time offices at the NCC. These cleared personnel have access to classified read binders and can interact with the NCC Watch on a 24-hour basis. Additionally, the NCC conducts weekly conference calls where members



interact with those Federal departments and agencies with the most significant communications responsibilities and requirements.

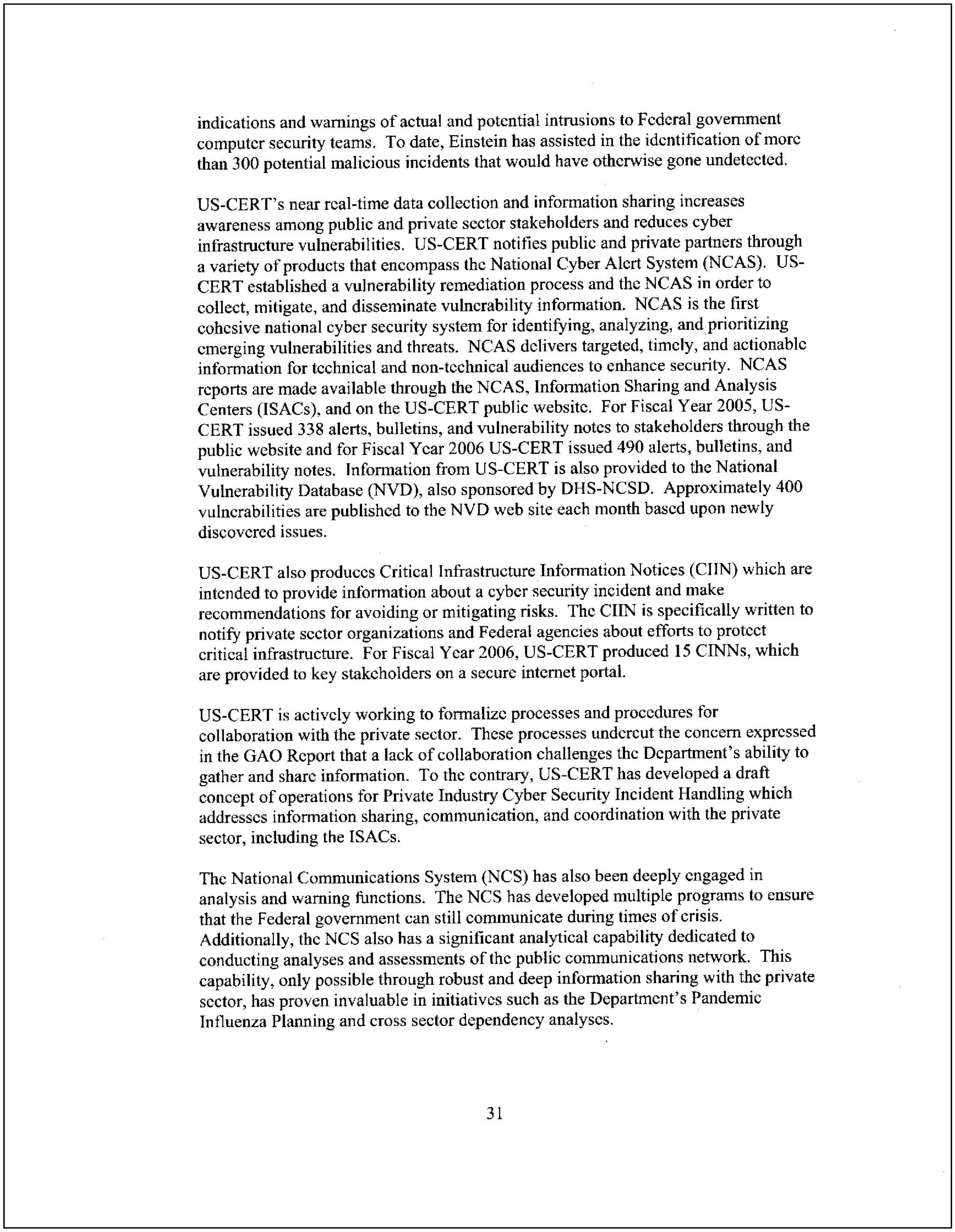
Moreover, explicitly excluded is an assessment of the private sector utilization of the HSIN. Consequently, the GAO Report does not accurately reflect the current deployment approach for the HSIN in the CI/KR sectors. Nine of the CI/KR sectors or major sub-sectors have signed memoranda of understanding with DHS to deploy Homeland Security Information Network-Critical Sectors (HSIN-CS) to their sectors.

Also, DHS strategic, operational, and policy initiatives have taken into account the critical role the private sector plays in protecting the Homeland. DHS has taken steps to designate a DHS Coordinator for Private Sector Security within DHS, who develops internal cross-cutting processes for synchronizing DHS efforts to support Private Sector security interests, and develop a way forward to expand and sustain the DHS/Private Sector partnership.

It appears the GAO Report largely relies on previous reports that do not account for the achievements discussed above and other recent successes. For example, in making its "Generally Not Achieved" assessment, the GAO Report cites assessments in an OIG report entitled, *Homeland Security Information Network Could Support Information Sharing More Effectively (OIG-06-38)*. However, in a letter dated July 11, 2007 from the OIG regarding the compliance follow-up to OIG-06-38, the Assistant Inspector General, Information Technology stated that five recommendations from the OIG report "are considered resolved." The OIG has also indicated that it is satisfied with DHS's efforts to mitigate problems outlined in the OIG-06-38 report.

***Performance Expectation 4****: Develop and enhance national analysis and warning capabilities for critical infrastructure.* The GAO Report – which focuses its assessment primarily on cyber critical infrastructure – does not give the Department credit for the significant advances it has made in achieving this performance expectation. In the area of cyber infrastructure, the GAO Report inaccurately suggests that the Department has provided no evidence of enhanced national warning capabilities. This assessment does not consider the tremendous progress by the Department's National Cyber Security Division (DHS-NCSD), within the Office of Cyber Security and Communications (DHS-CS&C), to develop and enhance cyber analysis, watch and warning, and collaboration with the private sector.

The U.S. Computer Emergency Readiness Team (US-CERT) within DHS-NCSD provides a 24-hour, 7 day-a-week watch center to conduct daily analysis and situational monitoring in order to provide information on cyber incidents and other events. For example, US-CERT's Einstein program enables the rapid detection of current and pending cyber attacks affecting agencies and provides federal agencies with early incident detection. The information gathered by the Einstein program is analyzed and then used to provide actionable and timely alerts and reporting regarding current and impending cyber attacks. The program also provides



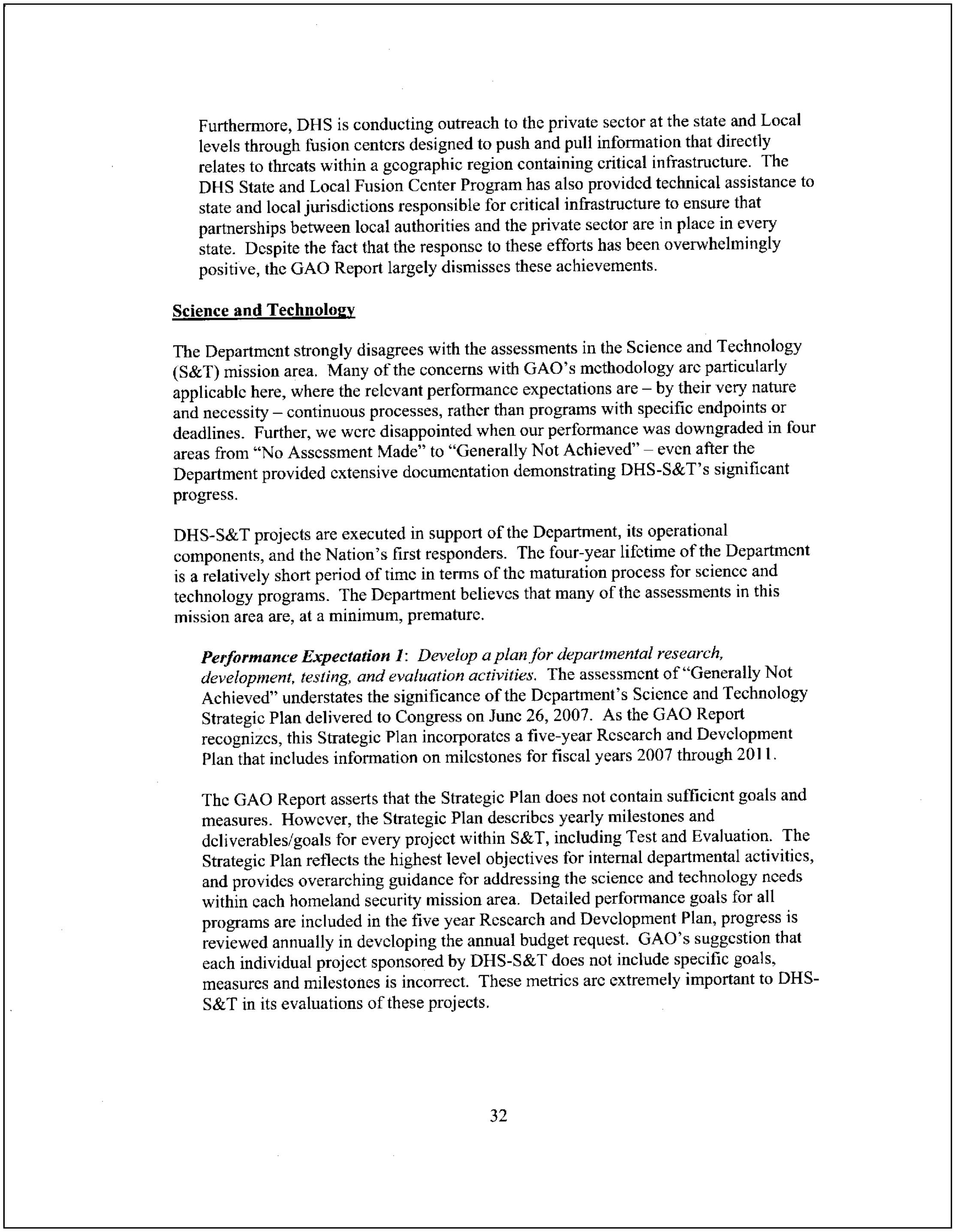
indications and warnings of actual and potential intrusions to Federal government computer security teams. To date, Einstein has assisted in the identification of more than 300 potential malicious incidents that would have otherwise gone undetected.

US-CERT's near real-time data collection and information sharing increases awareness among public and private sector stakeholders and reduces cyber infrastructure vulnerabilities. US-CERT notifies public and private partners through a variety of products that encompass the National Cyber Alert System (NCAS). US-CERT established a vulnerability remediation process and the NCAS in order to collect, mitigate, and disseminate vulnerability information. NCAS is the first cohesive national cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. NCAS delivers targeted, timely, and actionable information for technical and non-technical audiences to enhance security. NCAS reports are made available through the NCAS, Information Sharing and Analysis Centers (ISACs), and on the US-CERT public website. For Fiscal Year 2005, US-CERT issued 338 alerts, bulletins, and vulnerability notes to stakeholders through the public website and for Fiscal Year 2006 US-CERT issued 490 alerts, bulletins, and vulnerability notes. Information from US-CERT is also provided to the National Vulnerability Database (NVD), also sponsored by DHS-NCSD. Approximately 400 vulnerabilities are published to the NVD web site each month based upon newly discovered issues.

US-CERT also produces Critical Infrastructure Information Notices (CIIN) which are intended to provide information about a cyber security incident and make recommendations for avoiding or mitigating risks. The CIIN is specifically written to notify private sector organizations and Federal agencies about efforts to protect critical infrastructure. For Fiscal Year 2006, US-CERT produced 15 CINNs, which are provided to key stakeholders on a secure internet portal.

US-CERT is actively working to formalize processes and procedures for collaboration with the private sector. These processes undercut the concern expressed in the GAO Report that a lack of collaboration challenges the Department's ability to gather and share information. To the contrary, US-CERT has developed a draft concept of operations for Private Industry Cyber Security Incident Handling which addresses information sharing, communication, and coordination with the private sector, including the ISACs.

The National Communications System (NCS) has also been deeply engaged in analysis and warning functions. The NCS has developed multiple programs to ensure that the Federal government can still communicate during times of crisis. Additionally, the NCS also has a significant analytical capability dedicated to conducting analyses and assessments of the public communications network. This capability, only possible through robust and deep information sharing with the private sector, has proven invaluable in initiatives such as the Department's Pandemic Influenza Planning and cross sector dependency analyses.



Furthermore, DHS is conducting outreach to the private sector at the state and Local levels through fusion centers designed to push and pull information that directly relates to threats within a geographic region containing critical infrastructure. The DHS State and Local Fusion Center Program has also provided technical assistance to state and local jurisdictions responsible for critical infrastructure to ensure that partnerships between local authorities and the private sector are in place in every state. Despite the fact that the response to these efforts has been overwhelmingly positive, the GAO Report largely dismisses these achievements.

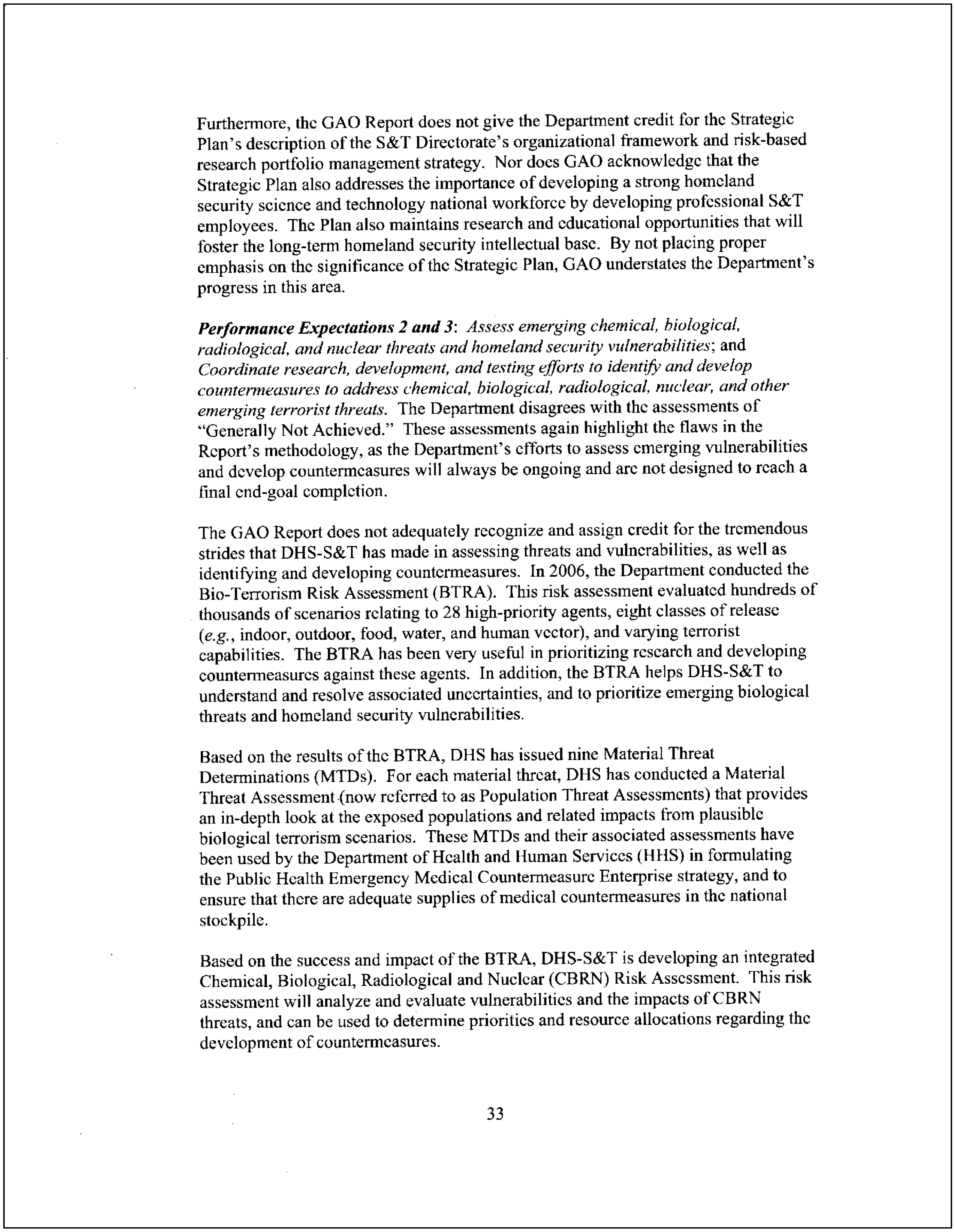
**Science and Technology**

The Department strongly disagrees with the assessments in the Science and Technology (S&T) mission area. Many of the concerns with GAO's methodology are particularly applicable here, where the relevant performance expectations are – by their very nature and necessity – continuous processes, rather than programs with specific endpoints or deadlines. Further, we were disappointed when our performance was downgraded in four areas from "No Assessment Made" to "Generally Not Achieved" – even after the Department provided extensive documentation demonstrating DHS-S&T's significant progress.

DHS-S&T projects are executed in support of the Department, its operational components, and the Nation's first responders. The four-year lifetime of the Department is a relatively short period of time in terms of the maturation process for science and technology programs. The Department believes that many of the assessments in this mission area are, at a minimum, premature.

***Performance Expectation 1****: Develop a plan for departmental research, development, testing, and evaluation activities.* The assessment of "Generally Not Achieved" understates the significance of the Department's Science and Technology Strategic Plan delivered to Congress on June 26, 2007. As the GAO Report recognizes, this Strategic Plan incorporates a five-year Research and Development Plan that includes information on milestones for fiscal years 2007 through 2011.

The GAO Report asserts that the Strategic Plan does not contain sufficient goals and measures. However, the Strategic Plan describes yearly milestones and deliverables/goals for every project within S&T, including Test and Evaluation. The Strategic Plan reflects the highest level objectives for internal departmental activities, and provides overarching guidance for addressing the science and technology needs within each homeland security mission area. Detailed performance goals for all programs are included in the five year Research and Development Plan, progress is reviewed annually in developing the annual budget request. GAO's suggestion that each individual project sponsored by DHS-S&T does not include specific goals, measures and milestones is incorrect. These metrics are extremely important to DHS-S&T in its evaluations of these projects.



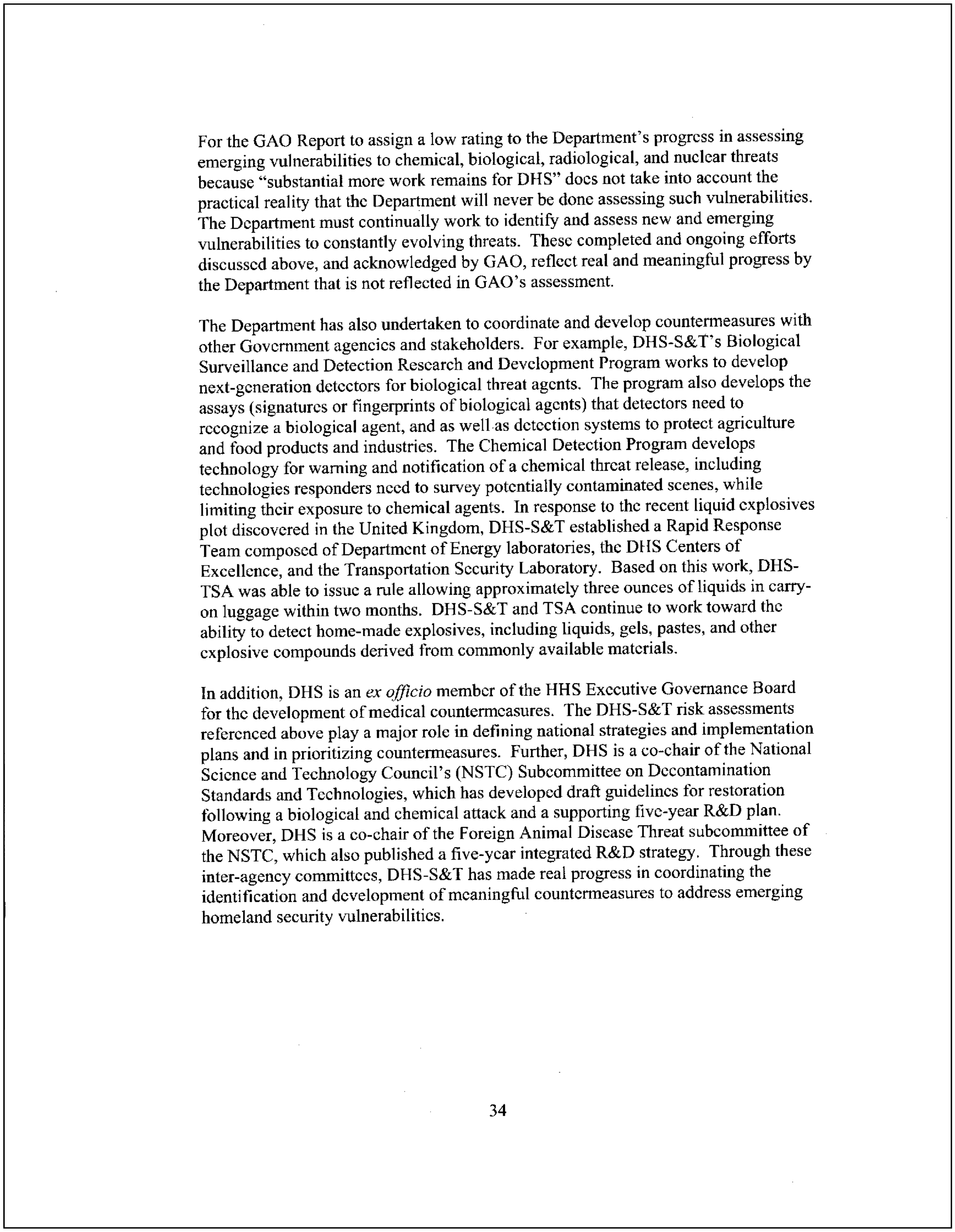
Furthermore, the GAO Report does not give the Department credit for the Strategic Plan's description of the S&T Directorate's organizational framework and risk-based research portfolio management strategy. Nor does GAO acknowledge that the Strategic Plan also addresses the importance of developing a strong homeland security science and technology national workforce by developing professional S&T employees. The Plan also maintains research and educational opportunities that will foster the long-term homeland security intellectual base. By not placing proper emphasis on the significance of the Strategic Plan, GAO understates the Department's progress in this area.

***Performance Expectations 2 and 3***: *Assess emerging chemical, biological, radiological, and nuclear threats and homeland security vulnerabilities*; and *Coordinate research, development, and testing efforts to identify and develop countermeasures to address chemical, biological, radiological, nuclear, and other emerging terrorist threats.* The Department disagrees with the assessments of "Generally Not Achieved." These assessments again highlight the flaws in the Report's methodology, as the Department's efforts to assess emerging vulnerabilities and develop countermeasures will always be ongoing and are not designed to reach a final end-goal completion.

The GAO Report does not adequately recognize and assign credit for the tremendous strides that DHS-S&T has made in assessing threats and vulnerabilities, as well as identifying and developing countermeasures. In 2006, the Department conducted the Bio-Terrorism Risk Assessment (BTRA). This risk assessment evaluated hundreds of thousands of scenarios relating to 28 high-priority agents, eight classes of release (*e.g.*, indoor, outdoor, food, water, and human vector), and varying terrorist capabilities. The BTRA has been very useful in prioritizing research and developing countermeasures against these agents. In addition, the BTRA helps DHS-S&T to understand and resolve associated uncertainties, and to prioritize emerging biological threats and homeland security vulnerabilities.

Based on the results of the BTRA, DHS has issued nine Material Threat Determinations (MTDs). For each material threat, DHS has conducted a Material Threat Assessment (now referred to as Population Threat Assessments) that provides an in-depth look at the exposed populations and related impacts from plausible biological terrorism scenarios. These MTDs and their associated assessments have been used by the Department of Health and Human Services (HHS) in formulating the Public Health Emergency Medical Countermeasure Enterprise strategy, and to ensure that there are adequate supplies of medical countermeasures in the national stockpile.

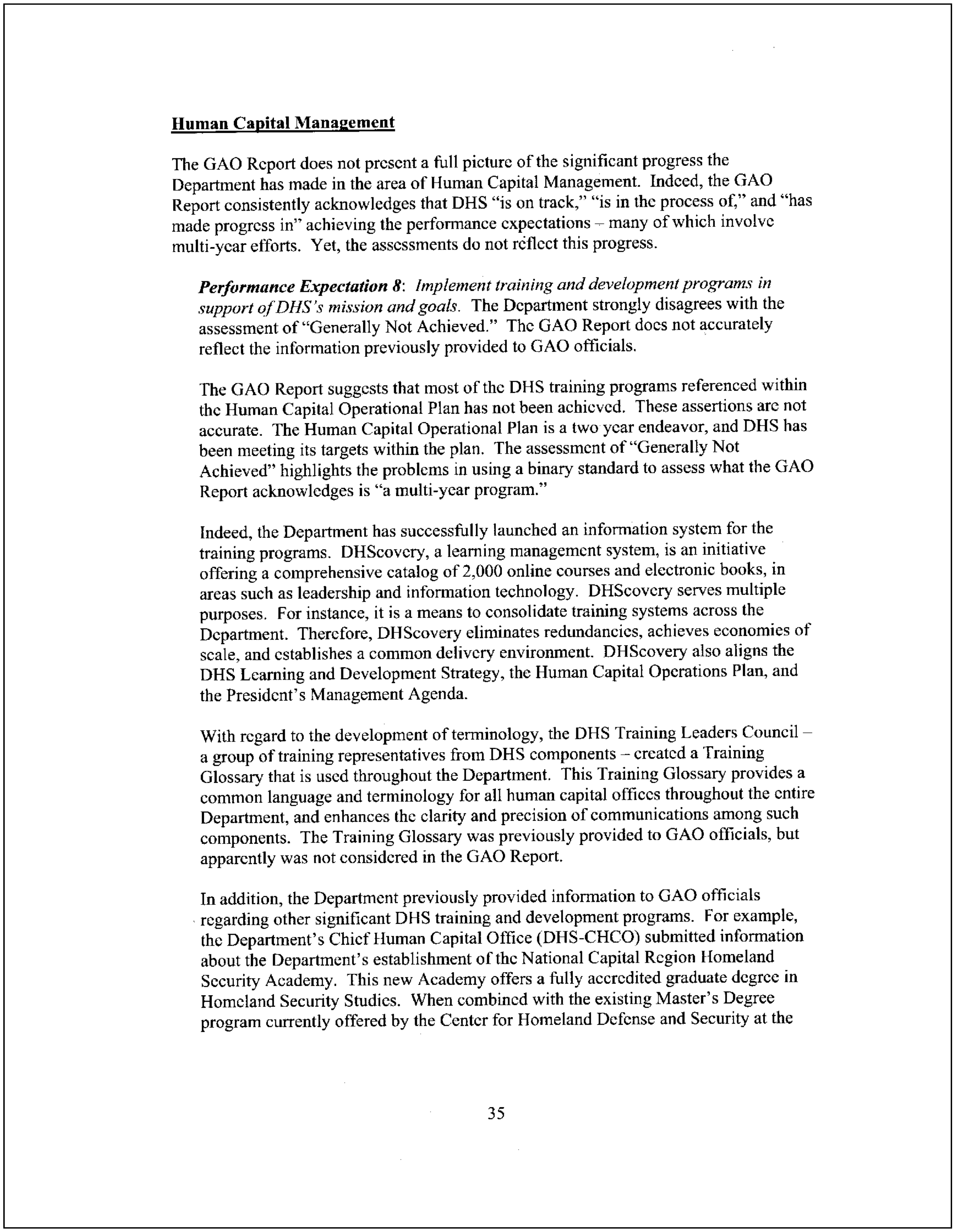
Based on the success and impact of the BTRA, DHS-S&T is developing an integrated Chemical, Biological, Radiological and Nuclear (CBRN) Risk Assessment. This risk assessment will analyze and evaluate vulnerabilities and the impacts of CBRN threats, and can be used to determine priorities and resource allocations regarding the development of countermeasures.



For the GAO Report to assign a low rating to the Department's progress in assessing emerging vulnerabilities to chemical, biological, radiological, and nuclear threats because "substantial more work remains for DHS" does not take into account the practical reality that the Department will never be done assessing such vulnerabilities. The Department must continually work to identify and assess new and emerging vulnerabilities to constantly evolving threats. These completed and ongoing efforts discussed above, and acknowledged by GAO, reflect real and meaningful progress by the Department that is not reflected in GAO's assessment.

The Department has also undertaken to coordinate and develop countermeasures with other Government agencies and stakeholders. For example, DHS-S&T's Biological Surveillance and Detection Research and Development Program works to develop next-generation detectors for biological threat agents. The program also develops the assays (signatures or fingerprints of biological agents) that detectors need to recognize a biological agent, and as well as detection systems to protect agriculture and food products and industries. The Chemical Detection Program develops technology for warning and notification of a chemical threat release, including technologies responders need to survey potentially contaminated scenes, while limiting their exposure to chemical agents. In response to the recent liquid explosives plot discovered in the United Kingdom, DHS-S&T established a Rapid Response Team composed of Department of Energy laboratories, the DHS Centers of Excellence, and the Transportation Security Laboratory. Based on this work, DHS-TSA was able to issue a rule allowing approximately three ounces of liquids in carry-on luggage within two months. DHS-S&T and TSA continue to work toward the ability to detect home-made explosives, including liquids, gels, pastes, and other explosive compounds derived from commonly available materials.

In addition, DHS is an *ex officio* member of the HHS Executive Governance Board for the development of medical countermeasures. The DHS-S&T risk assessments referenced above play a major role in defining national strategies and implementation plans and in prioritizing countermeasures. Further, DHS is a co-chair of the National Science and Technology Council's (NSTC) Subcommittee on Decontamination Standards and Technologies, which has developed draft guidelines for restoration following a biological and chemical attack and a supporting five-year R&D plan. Moreover, DHS is a co-chair of the Foreign Animal Disease Threat subcommittee of the NSTC, which also published a five-year integrated R&D strategy. Through these inter-agency committees, DHS-S&T has made real progress in coordinating the identification and development of meaningful countermeasures to address emerging homeland security vulnerabilities.



**Human Capital Management**

The GAO Report does not present a full picture of the significant progress the Department has made in the area of Human Capital Management. Indeed, the GAO Report consistently acknowledges that DHS "is on track," "is in the process of," and "has made progress in" achieving the performance expectations – many of which involve multi-year efforts. Yet, the assessments do not reflect this progress.

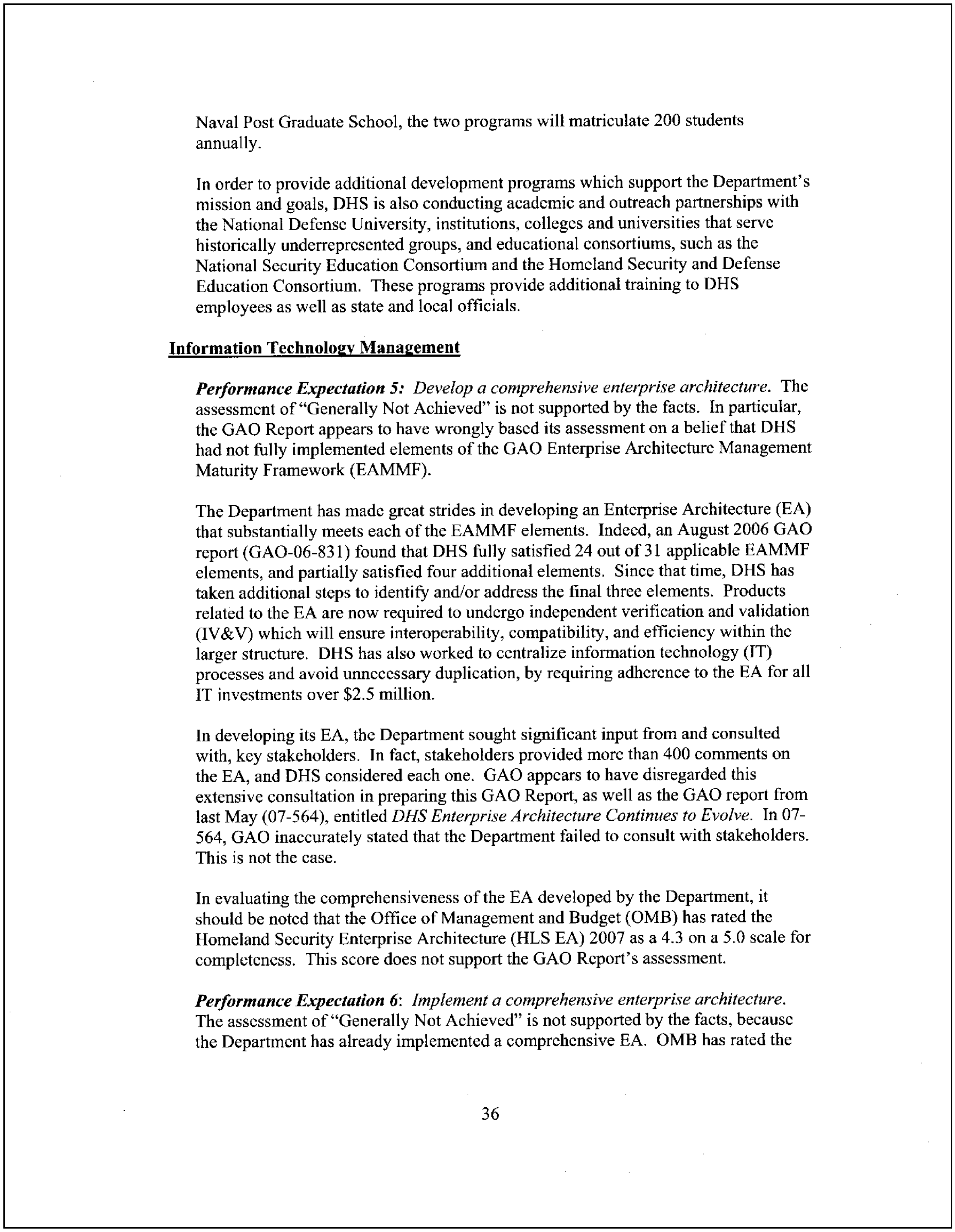
***Performance Expectation 8***: *Implement training and development programs in support of DHS's mission and goals.* The Department strongly disagrees with the assessment of "Generally Not Achieved." The GAO Report does not accurately reflect the information previously provided to GAO officials.

The GAO Report suggests that most of the DHS training programs referenced within the Human Capital Operational Plan has not been achieved. These assertions are not accurate. The Human Capital Operational Plan is a two year endeavor, and DHS has been meeting its targets within the plan. The assessment of "Generally Not Achieved" highlights the problems in using a binary standard to assess what the GAO Report acknowledges is "a multi-year program."

Indeed, the Department has successfully launched an information system for the training programs. DHScovery, a learning management system, is an initiative offering a comprehensive catalog of 2,000 online courses and electronic books, in areas such as leadership and information technology. DHScovery serves multiple purposes. For instance, it is a means to consolidate training systems across the Department. Therefore, DHScovery eliminates redundancies, achieves economies of scale, and establishes a common delivery environment. DHScovery also aligns the DHS Learning and Development Strategy, the Human Capital Operations Plan, and the President's Management Agenda.

With regard to the development of terminology, the DHS Training Leaders Council – a group of training representatives from DHS components – created a Training Glossary that is used throughout the Department. This Training Glossary provides a common language and terminology for all human capital offices throughout the entire Department, and enhances the clarity and precision of communications among such components. The Training Glossary was previously provided to GAO officials, but apparently was not considered in the GAO Report.

In addition, the Department previously provided information to GAO officials regarding other significant DHS training and development programs. For example, the Department's Chief Human Capital Office (DHS-CHCO) submitted information about the Department's establishment of the National Capital Region Homeland Security Academy. This new Academy offers a fully accredited graduate degree in Homeland Security Studies. When combined with the existing Master's Degree program currently offered by the Center for Homeland Defense and Security at the



Naval Post Graduate School, the two programs will matriculate 200 students annually.

In order to provide additional development programs which support the Department's mission and goals, DHS is also conducting academic and outreach partnerships with the National Defense University, institutions, colleges and universities that serve historically underrepresented groups, and educational consortiums, such as the National Security Education Consortium and the Homeland Security and Defense Education Consortium. These programs provide additional training to DHS employees as well as state and local officials.

**Information Technology Management**

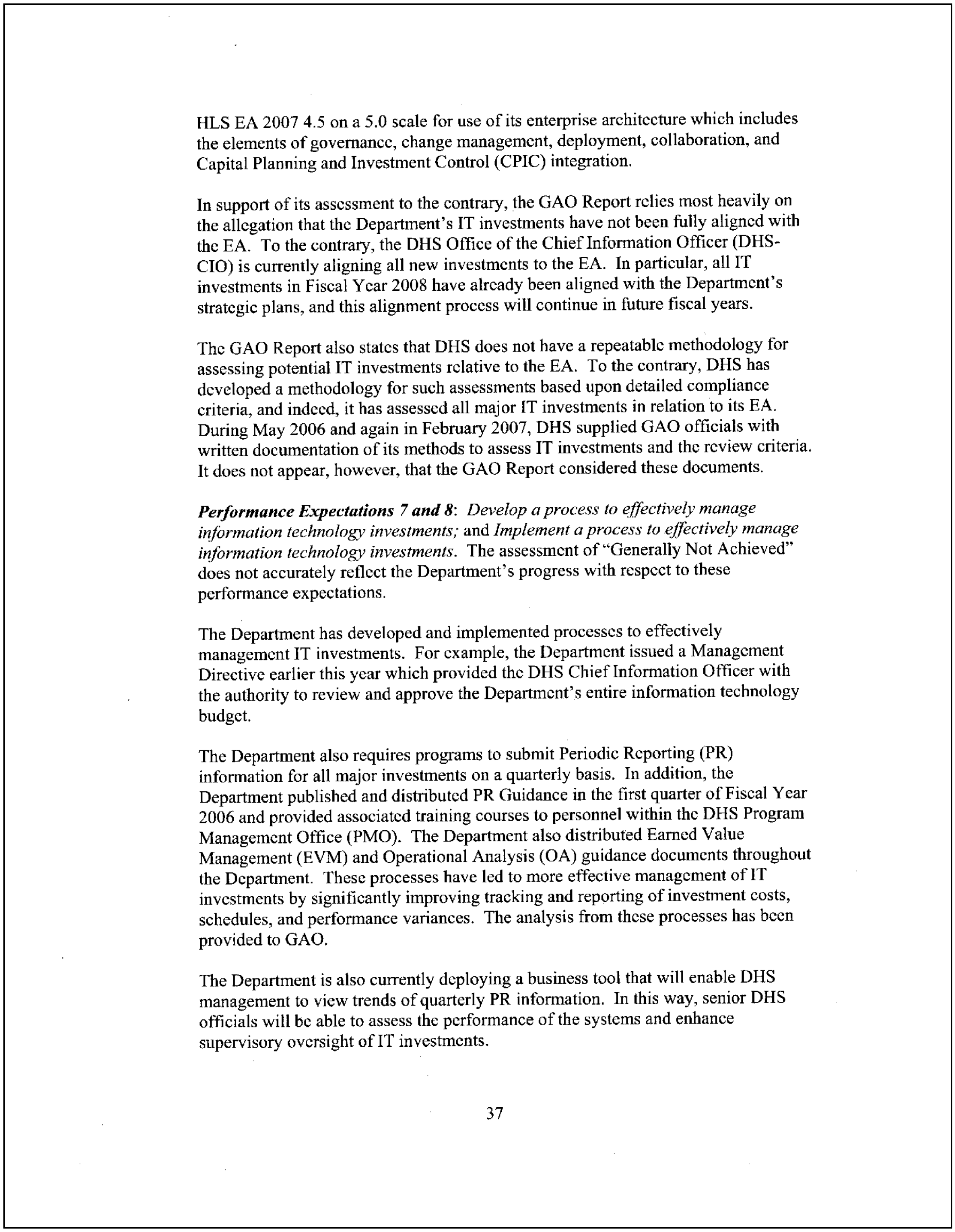
***Performance Expectation 5:*** *Develop a comprehensive enterprise architecture.* The assessment of "Generally Not Achieved" is not supported by the facts. In particular, the GAO Report appears to have wrongly based its assessment on a belief that DHS had not fully implemented elements of the GAO Enterprise Architecture Management Maturity Framework (EAMMF).

The Department has made great strides in developing an Enterprise Architecture (EA) that substantially meets each of the EAMMF elements. Indeed, an August 2006 GAO report (GAO-06-831) found that DHS fully satisfied 24 out of 31 applicable EAMMF elements, and partially satisfied four additional elements. Since that time, DHS has taken additional steps to identify and/or address the final three elements. Products related to the EA are now required to undergo independent verification and validation (IV&V) which will ensure interoperability, compatibility, and efficiency within the larger structure. DHS has also worked to centralize information technology (IT) processes and avoid unnecessary duplication, by requiring adherence to the EA for all IT investments over $2.5 million.

In developing its EA, the Department sought significant input from and consulted with, key stakeholders. In fact, stakeholders provided more than 400 comments on the EA, and DHS considered each one. GAO appears to have disregarded this extensive consultation in preparing this GAO Report, as well as the GAO report from last May (07-564), entitled *DHS Enterprise Architecture Continues to Evolve*. In 07-564, GAO inaccurately stated that the Department failed to consult with stakeholders. This is not the case.

In evaluating the comprehensiveness of the EA developed by the Department, it should be noted that the Office of Management and Budget (OMB) has rated the Homeland Security Enterprise Architecture (HLS EA) 2007 as a 4.3 on a 5.0 scale for completeness. This score does not support the GAO Report's assessment.

***Performance Expectation 6***: *Implement a comprehensive enterprise architecture.* The assessment of "Generally Not Achieved" is not supported by the facts, because the Department has already implemented a comprehensive EA. OMB has rated the



HLS EA 2007 4.5 on a 5.0 scale for use of its enterprise architecture which includes the elements of governance, change management, deployment, collaboration, and Capital Planning and Investment Control (CPIC) integration.

In support of its assessment to the contrary, the GAO Report relies most heavily on the allegation that the Department's IT investments have not been fully aligned with the EA. To the contrary, the DHS Office of the Chief Information Officer (DHS-CIO) is currently aligning all new investments to the EA. In particular, all IT investments in Fiscal Year 2008 have already been aligned with the Department's strategic plans, and this alignment process will continue in future fiscal years.

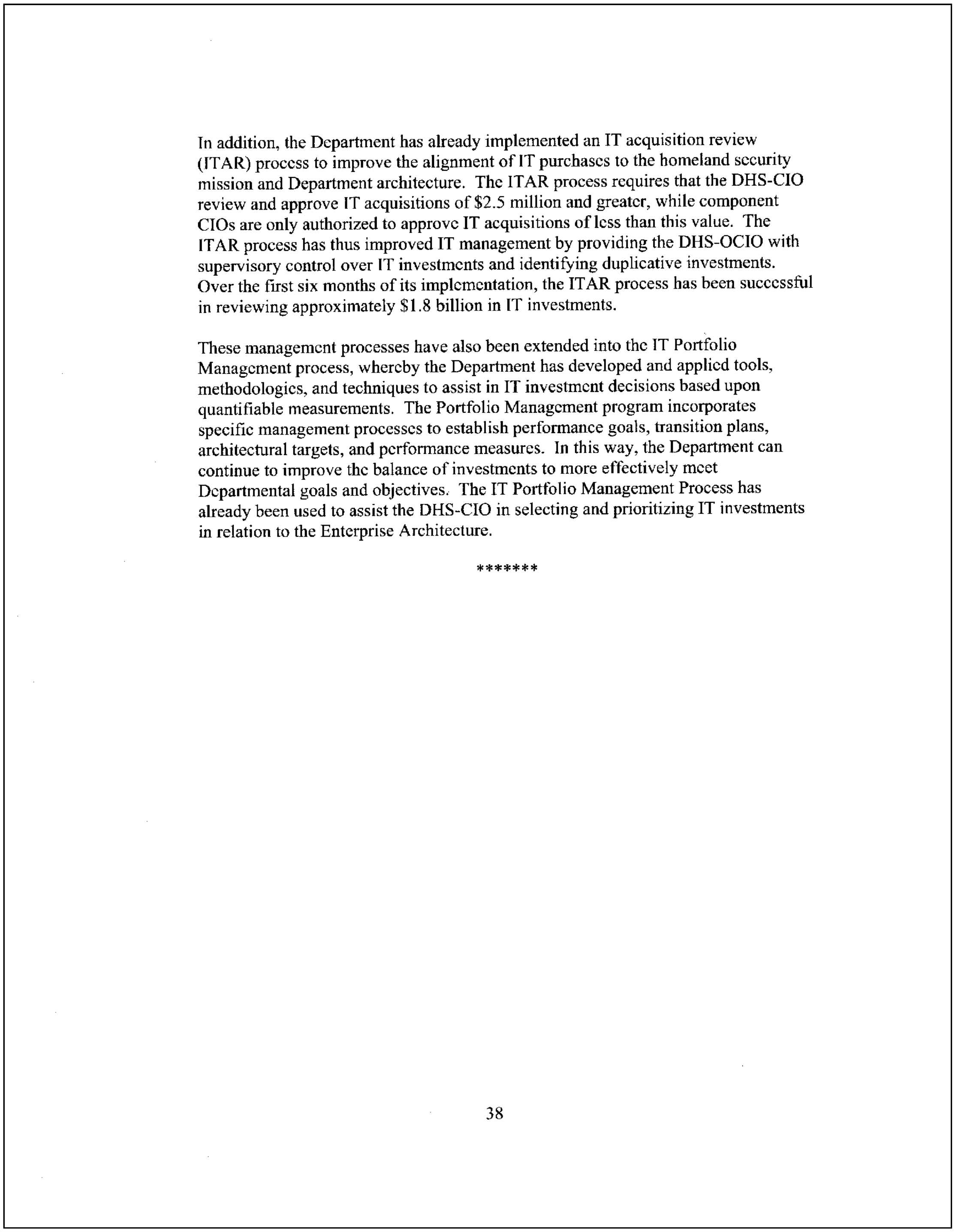
The GAO Report also states that DHS does not have a repeatable methodology for assessing potential IT investments relative to the EA. To the contrary, DHS has developed a methodology for such assessments based upon detailed compliance criteria, and indeed, it has assessed all major IT investments in relation to its EA. During May 2006 and again in February 2007, DHS supplied GAO officials with written documentation of its methods to assess IT investments and the review criteria. It does not appear, however, that the GAO Report considered these documents.

***Performance Expectations 7 and 8***: *Develop a process to effectively manage information technology investments;* and *Implement a process to effectively manage information technology investments*. The assessment of "Generally Not Achieved" does not accurately reflect the Department's progress with respect to these performance expectations.

The Department has developed and implemented processes to effectively management IT investments. For example, the Department issued a Management Directive earlier this year which provided the DHS Chief Information Officer with the authority to review and approve the Department's entire information technology budget.

The Department also requires programs to submit Periodic Reporting (PR) information for all major investments on a quarterly basis. In addition, the Department published and distributed PR Guidance in the first quarter of Fiscal Year 2006 and provided associated training courses to personnel within the DHS Program Management Office (PMO). The Department also distributed Earned Value Management (EVM) and Operational Analysis (OA) guidance documents throughout the Department. These processes have led to more effective management of IT investments by significantly improving tracking and reporting of investment costs, schedules, and performance variances. The analysis from these processes has been provided to GAO.

The Department is also currently deploying a business tool that will enable DHS management to view trends of quarterly PR information. In this way, senior DHS officials will be able to assess the performance of the systems and enhance supervisory oversight of IT investments.



In addition, the Department has already implemented an IT acquisition review (ITAR) process to improve the alignment of IT purchases to the homeland security mission and Department architecture. The ITAR process requires that the DHS-CIO review and approve IT acquisitions of $2.5 million and greater, while component CIOs are only authorized to approve IT acquisitions of less than this value. The ITAR process has thus improved IT management by providing the DHS-OCIO with supervisory control over IT investments and identifying duplicative investments. Over the first six months of its implementation, the ITAR process has been successful in reviewing approximately $1.8 billion in IT investments.

These management processes have also been extended into the IT Portfolio Management process, whereby the Department has developed and applied tools, methodologies, and techniques to assist in IT investment decisions based upon quantifiable measurements. The Portfolio Management program incorporates specific management processes to establish performance goals, transition plans, architectural targets, and performance measures. In this way, the Department can continue to improve the balance of investments to more effectively meet Departmental goals and objectives. The IT Portfolio Management Process has already been used to assist the DHS-CIO in selecting and prioritizing IT investments in relation to the Enterprise Architecture.

*******

# Appendix III: GAO Contact and Staff Acknowledgments

## GAO Contact

Norman J. Rabkin (202) 512-8777 or rabkinn@gao.gov

## Staff Acknowledgments

In addition to the person named above, Christopher Keisling, Assistant Director; Jason Barnosky; Cathleen A. Berrick; Sharon Caudle; Virginia Chanley; Michele Fejfar; Rebecca Gambler; Kathryn Godfrey; Stephanie Hockman; Tracey King; Thomas Lombardi; Jan Montgomery; Octavia Parks; and Sue Ramanathan made key contributions to this report. Other contributors to this report included Eugene Aloise; John Bagnulo; Mark Bird; Nancy Briggs; Kristy Brown; Stephen Caldwell; Frances Cook; Stephen Donahue; Jeanette Espinola; Jess Ford; Amanda Gill; Mark Goldstein; Ellen Grady; Samuel Hinojosa; Randolph Hite; Daniel Hoy; John Hutton; William O. Jenkins, Jr.; Casey Keplinger; Kirk Kiester; Eileen Larence; Leena Mathew; Kieran McCarthy; Tiffany Mostert; Shannin O'Neill; Bonita Oden; David Powner; Jerry Seigler; Katherine Siggerud; Richard Stana; Bernice Steinhardt; John Stephenson; Sarah Veale; John Vocino; Gregory Wilshusen; Eugene Wisnoksi; and William T. Woods.

# Related GAO Products

## Border Security

*Homeland Security: Prospects For Biometric US-VISIT Exit Capability Remain Unclear.* GAO-07-1044T. Washington, D.C.: June 28, 2007.

*Border Patrol: Costs and Challenges Related to Training New Agents.* GAO-07-997T. Washington, D.C.: June 19, 2007.

*Homeland Security: Information on Training New Border Patrol Agents.* GAO-07-540R. Washington, D.C.: March 30, 2007.

*Homeland Security: US-VISIT Program Faces Operational, Technological, and Management Challenges.* GAO-07-632T. Washington, D.C.: March 20, 2007.

*Secure Border Initiative: SBI*net *Planning and Management Improvements Needed to Control Risks.* GAO-07-504T. Washington, D.C.: February 27, 2007.

*Homeland Security: US-VISIT Has Not Fully Met Expectations and Longstanding Program Management Challenges Need to Be Addressed.* GAO-07-499T. Washington, D.C.: February 16, 2007.

*Secure Border Initiative: SBI*net *Expenditure Plan Needs to Better Support Oversight and Accountability.* GAO-07-309. Washington, D.C.: February 15, 2007.

*Homeland Security: Planned Expenditures for U.S. Visitor and Immigrant Status Program Need to Be Adequately Defined and Justified.* GAO-07-278. Washington, D.C.: February 14, 2007.

*Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry.* GAO-07-378T. Washington, D.C.: January 31, 2007.

*Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry.* GAO-07-248. Washington, D.C.: December 6, 2006.

*Department of Homeland Security and Department of State: Documents Required for Travelers Departing From or Arriving in the United States at Air Ports-of-Entry From Within the Western Hemisphere.* GAO-07-250R. Washington, DC: December 6, 2006.

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

*Illegal Immigration: Border-Crossing Deaths Have Doubled Since 1995; Border Patrol's Efforts to Prevent Deaths Have Not Been Fully Evaluated.* GAO-06-770. Washington, D.C.: August 15, 2006.

*Border Security: Continued Weaknesses in Screening Entrants into the United States.* GAO-06-976T. Washington, D.C.: August 2, 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.

*Process for Admitting Additional Countries into the Visa Waiver Program.* GAO-06-835R. Washington, D.C.: July 28, 2006.

*Intellectual Property: Initial Observations on the STOP Initiative and U.S. Border Efforts to Reduce Piracy.* GAO-06-1004T. Washington, D.C.: July 26, 2006.

*Border Security: Investigators Transported Radioactive Sources Across Our Nation's Borders at Two Locations.* GAO-06-940T. Washington, D.C.: July 7, 2006.

*Border Security: Investigators Transported Radioactive Sources Across Our Nation's Borders at Two Locations.* GAO-06-939T. Washington, D.C.: July 5, 2006.

*Information on Immigration Enforcement and Supervisory Promotions in the Department of Homeland Security's Immigration and Customs Enforcement and Customs and Border Protection.* GAO-06-751R. Washington, D.C.: June 13, 2006.

*Homeland Security: Contract Management and Oversight for Visitor and Immigrant Status Program Need to Be Strengthened.* GAO-06-404. Washington, D.C.: June 9, 2006.

*Observations on Efforts to Implement the Western Hemisphere Travel Initiative on the U.S. Border with Canada.* GAO-06-741R. Washington, D.C.: May 25, 2006.

*Homeland Security: Management and Coordination Problems Increase the Vulnerability of U.S. Agriculture to Foreign Pests and Disease.* GAO-06-644. Washington, D.C.: May 19, 2006.

*Border Security: Reassessment of Consular Resource Requirements Could Help Address Visa Delays.* GAO-06-542T. Washington, D.C.: April 4, 2006.

*Border Security: Investigators Transported Radioactive Sources Across Our Nation's Borders at Two Locations.* GAO-06-583T. Washington, D.C.: March 28, 2006.

*Border Security: Investigators Successfully Transported Radioactive Sources Across Our Nation's Borders at Selected Locations.* GAO-06-545R. Washington, D.C.: March 28, 2006.

*Homeland Security: Better Management Practices Could Enhance DHS's Ability to Allocate Investigative Resources.* GAO-06-462T. Washington, D.C.: March 28, 2006.

*Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports-of-Entry, but Concerns Remain.* GAO-06-389. Washington, D.C.: March 22, 2006.

*Combating Nuclear Smuggling: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries.* GAO-06-311. Washington, D.C.: March 14, 2006.

*Border Security: Key Unresolved Issues Justify Reevaluation of Border Surveillance Technology Program.* GAO-06-295. Washington, D.C.: February 22, 2006.

*Homeland Security: Recommendations to Improve Management of Key Border Security Program Need to Be Implemented.* GAO-06-296. Washington, D.C.: February 14, 2006.

*Homeland Security: Visitor and Immigrant Status Program Operating, but Management Improvements Are Still Needed.* GAO-06-318T. Washington, D.C.: January 25, 2006.

*Border Security: Strengthened Visa Process Would Benefit from Improvements in Staffing and Information Sharing.* GAO-05-859. Washington, D.C.: September 13, 2005.

*Border Security: Opportunities to Increase Coordination of Air and Marine Assets.* GAO-05-543. Washington, D.C.: August 12, 2005.

*Border Security: Actions Needed to Strengthen Management of Department of Homeland Security's Visa Security Program.* GAO-05-801. Washington, D.C.: July 29, 2005.

*Border Patrol: Available Data on Interior Checkpoints Suggest Differences in Sector Performance.* GAO-05-435. Washington, D.C.: July 22, 2005.

*Combating Nuclear Smuggling: Efforts to Deploy Radiation Detection Equipment in the United States and in Other Countries.* GAO-05-840T. Washington, D.C.: June 21, 2005.

*Homeland Security: Performance of Foreign Student and Exchange Visitor Information System Continues to Improve, But Issues Remain.* GAO-05-440T. Washington, D.C.: March 17, 2005.

*Homeland Security: Some Progress Made, but Many Challenges Remain on U.S. Visitor and Immigrant Status Indicator Technology Program.* GAO-05-202. Washington, D.C.: February 23, 2005.

*Border Security: Streamlined Visas Mantis Program Has Lowered Burden on Foreign Science Students and Scholars, but Further Refinements Needed.* GAO-05-198. Washington, D.C.: February 18, 2005.

*Border Security: Joint, Coordinated Actions by State and DHS Needed to Guide Biometric Visas and Related Programs.* GAO-04-1080T. Washington, D.C.: September 9, 2004.

*Border Security: State Department Rollout of Biometric Visas on Schedule, but Guidance Is Lagging.* GAO-04-1001. Washington, D.C.: September 9, 2004.

*Border Security: Consular Identification Cards Accepted within United States, but Consistent Federal Guidance Needed.* GAO-04-881. Washington, D.C.: August 24, 2004.

*Border Security: Additional Actions Needed to Eliminate Weaknesses in the Visa Revocation Process.* GAO-04-795. Washington, D.C.: July 13, 2004.

*Border Security: Additional Actions Needed to Eliminate Weaknesses in the Visa Revocation Process.* GAO-04-899T. Washington, D.C.: July 13, 2004.

*Border Security: Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands.* GAO-04-590. Washington, D.C.: June 16, 2004.

*Overstay Tracking: A Key Component of Homeland Security and a Layered Defense.* GAO-04-82. Washington, D.C.: May 21, 2004.

*Homeland Security: First Phase of Visitor and Immigration Status Program Operating, but Improvements Needed.* GAO-04-586. Washington, D.C.: May 11, 2004.

*Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed.* GAO-04-569T. Washington, D.C.: March 18, 2004.

*Border Security: Improvements Needed to Reduce Time Taken to Adjudicate Visas for Science Students and Scholars.* GAO-04-443T. Washington, D.C.: February 25, 2004.

*Border Security: Improvements Needed to Reduce Time Taken to Adjudicate Visas for Science Students and Scholars.* GAO-04-371. Washington, D.C.: February 25, 2004.

*Homeland Security: Overstay Tracking Is a Key Component of a Layered Defense.* GAO-04-170T. Washington, D.C.: October 16, 2003.

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

*Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed.* GAO-03-1083. Washington, D.C.: September 19, 2003.

*Security: Counterfeit Identification and Identification Fraud Raise Security Concerns.* GAO-03-1147T. Washington, D.C.: September 9, 2003.

*Land Border Ports of Entry: Vulnerabilities and Inefficiencies in the Inspections Process.* GAO-03-1084R. Washington, D.C.: August 18, 2003.

*Federal Law Enforcement Training Center: Capacity Planning and Management Oversight Need Improvement.* GAO-03-736. Washington, D.C.: July 24, 2003.

*Border Security: New Policies and Increased Interagency Coordination Needed to Improve Visa Process.* GAO-03-1013T. Washington, D.C.: July 15, 2003.

*Border Security: New Policies and Procedures Are Needed to Fill Gaps in the Visa Revocation Process.* GAO-03-908T. Washington, D.C.: June 18, 2003.

*Border Security: New Policies and Procedures Are Needed to Fill Gaps in the Visa Revocation Process.* GAO-03-798. Washington, D.C.: June 18, 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.

*Counterfeit Documents Used to Enter the United States From Certain Western Hemisphere Countries Not Detected.* GAO-03-713T. Washington, D.C.: May 13, 2003.

*Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing.* GAO-03-322. Washington, D.C.: April 15, 2003.

*Border Security: Challenges in Implementing Border Technology.* GAO-03-546T. Washington, D.C.: March 12, 2003.

## Immigration Enforcement

*Alien Detention Standards: Telephone Access Problems Were Pervasive at Detention Facilities; Other Deficiencies Did Not Show a Pattern of Noncompliance.* GAO-07-875. Washington, D.C.: July 6, 2007.

*Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Verification System.* GAO-07-924T. Washington, D.C.: June 7, 2007.

*Foreign Workers: Information on Selected Countries' Experiences.* GAO-06-1055. Washington, D.C.: September 8, 2006.

*Information Technology: Immigration and Customs Enforcement Is Beginning to Address Infrastructure Modernization Program Weaknesses, but Key Improvements Still Needed.* GAO-06-823. Washington, D.C.: July 27, 2006.

*Immigration Enforcement: Benefits and Limitations to Using Earnings Data to Identify Unauthorized Work.* GAO-06-814R. Washington, D.C.: July 11, 2006.

*Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts.* GAO-06-895T. Washington, D.C.: June 19, 2006.

*Information on Immigration Enforcement and Supervisory Promotions in the Department of Homeland Security's Immigration and Customs Enforcement and Customs and Border Protection.* GAO-06-751R. Washington, D.C.: June 13, 2006.

*Homeland Security: Better Management Practices Could Enhance DHS's Ability to Allocate Investigative Resources.* GAO-06-462T. Washington, D.C.: March 28, 2006.

*Information Technology: Management Improvements Needed on Immigration and Customs Enforcement's Infrastructure Modernization Program.* GAO-05-805. Washington, D.C.: September 7, 2005.

*Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts.* GAO-05-813. Washington, D.C.: August 31, 2005.

*Combating Alien Smuggling: The Federal Response Can Be Improved.* GAO-05-892T. Washington, D.C.: July 12, 2005.

*Combating Alien Smuggling: Opportunities Exist to Improve the Federal Response.* GAO-05-305. Washington, D.C.: May 27, 2005.

*Information on Certain Illegal Aliens Arrested in the United States.* GAO-05-646R. Washington, D.C.: May 9, 2005.

*Department of Homeland Security: Addressing Management Challenges that Face Immigration Enforcement Agencies.* GAO-05-664T. Washington, D.C.: May 5, 2005.

*Information on Criminal Aliens Incarcerated in Federal and State Prisons and Local Jails.* GAO-05-337R. Washington, D.C.: April 7, 2005.

*Homeland Security: Performance of Foreign Student and Exchange Visitor Information System Continues to Improve, But Issues Remain.* GAO-05-440T. Washington, D.C.: March 17, 2005.

*Alien Registration: Usefulness of a Nonimmigrant Alien Annual Address Reporting Requirement Is Questionable.* GAO-05-204. Washington, D.C.: January 28, 2005.

*Homeland Security: Management Challenges Remain in Transforming Immigration Programs.* GAO-05-81. Washington, D.C.: October 14, 2004.

*Immigration Enforcement: DHS Has Incorporated Immigration Enforcement Objectives and Is Addressing Future Planning Requirements.* GAO-05-66. Washington, D.C.: October 8, 2004.

*Homeland Security: Performance of Information System to Monitor Foreign Students and Exchange Visitors Has Improved, but Issues Remain.* GAO-04-690. Washington, D.C.: June 18, 2004.

*Investigations of Terrorist Financing, Money Laundering, and Other Financial Crimes.* GAO-04-464R. Washington, D.C.: February 20, 2004.

*Combating Money Laundering: Opportunities Exist to Improve the National Strategy.* GAO-03-813. Washington, D.C.: September 26, 2003.

## Immigration Services

*Department of Homeland Security: Adjustment of the Immigration and Naturalization Benefit Application and Petition Fee Schedule.* GAO-07-946R. Washington, D.C.: June 15, 2007.

*Immigration Benefits: Sixteenth Report Required by the Haitian Refugee Immigration Fairness Act of 1998.* GAO-07-796R. Washington, D.C.: April 27, 2007.

*DHS Immigration Attorneys: Workload Analysis and Workforce Planning Efforts Lack Data and Documentation.* GAO-07-206. Washington, D.C.: April 17, 2007.

*Foreign Physicians: Data on Use of J-1 Visa Waivers Needed to Better Address Physician Shortages.* GAO-07-52. Washington, D.C.: November 30, 2006.

*Immigration Benefits: Fifteenth Report Required by the Haitian Refugee Immigration Fairness Act of 1998.* GAO-07-168R. Washington, D.C.: November 9, 2006.

*Immigration Benefits: Additional Efforts Needed to Help Ensure Alien Files Are Located when Needed.* GAO-07-85. Washington, D.C.: October 27, 2006.

*Estimating the Undocumented Population: A "Grouped Answers" Approach to Surveying Foreign-Born Respondents.* GAO-06-775. Washington, D.C.: September 29, 2006.

*Executive Office for Immigration Review: Caseload Performance Reporting Needs Improvement.* GAO-06-771. Washington, D.C.: August 11, 2006.

*H-1B Visa Program: More Oversight by Labor Can Improve Compliance with Program Requirements.* GAO-06-901T. Washington, D.C.: June 22, 2006.

*H-1B Visa Program: Labor Could Improve Its Oversight and Increase Information Sharing with Homeland Security.* GAO-06-720. Washington, D.C.: June 22, 2006.

*Immigration Benefits: Circumstances under Which Petitioners' Sex Offenses May Be Disclosed to Beneficiaries.* GAO-06-735. Washington, D.C.: June 14, 2006.

*Immigration Benefits: Fourteenth Report Required by the Haitian Refugee Immigration Fairness Act of 1998.* GAO-06-589R. Washington, D.C.: April 21, 2006.

*Information Technology: Near-Term Effort to Automate Paper-Based Immigration Files Needs Planning Improvements.* GAO-06-375. Washington, D.C.: March 31, 2006.

*International Remittances: Different Estimation Methodologies Produce Different Results.* GAO-06-210. Washington, D.C.: March 28, 2006.

*Immigration Benefits: Additional Controls and a Sanctions Strategy Could Enhance DHS' Ability to Control Benefit Fraud.* GAO-06-259. Washington, D.C.: March 10, 2006.

*Social Security Administration: Procedures for Issuing Numbers and Benefits to the Foreign-Born.* GAO-06-253T. Washington, D.C.: March 2, 2006.

*Immigration Benefits: Improvements Needed to Address Backlogs and Ensure Quality of Adjudications.* GAO-06-20. Washington, D.C.: November 21, 2005.

*Immigration Benefits: Thirteenth Report Required by the Haitian Refugee Immigration Fairness Act of 1998.* GAO-06-122R. Washington, D.C.: October 21, 2005.

*Taxpayer Information: Options Exist to Enable Data Sharing Between IRS and USCIS but Each Presents Challenges.* GAO-06-100. Washington, D.C.: October 11, 2005.

*Immigration Services: Better Contracting Practices Needed at Call Centers.* GAO-05-526. Washington, D.C.: June 30, 2005.

*Immigration Benefits: Twelfth Report Required by the Haitian Refugee Immigration Fairness Act of 1998.* GAO-05-481R. Washington, D.C.: April 14, 2005.

*Immigrant Investors: Small Number of Participants Attributed to Pending Regulations and Other Factors.* GAO-05-256. Washington, D.C.: April 1, 2005.

*Immigration Benefits: Eleventh Report Required by the Haitian Refugee Immigration Fairness Act of 1998.* GAO-04-1030R. Washington, D.C.: August 13, 2004.

*Taxpayer Information: Data Sharing and Analysis May Enhance Tax Compliance and Improve Immigration Eligibility Decisions.* GAO-04-972T. Washington, D.C.: July 21, 2004.

*Illegal Alien Schoolchildren: Issues in Estimating State-by-State Costs.* GAO-04-733. Washington, D.C.: June 21, 2004.

*Undocumented Aliens: Questions Persist about Their Impact on Hospitals' Uncompensated Care Costs.* GAO-04-472. Washington, D.C.: May 21, 2004.

*Immigration Application Fees: Current Fees Are Not Sufficient to Fund U.S. Citizenship and Immigration Services' Operations.* GAO-04-309R. Washington, D.C.: January 5, 2004.

*Immigration Benefits: Tenth Report Required by the Haitian Refugee Immigration Fairness Act of 1998.* GAO-04-189R. Washington, D.C.: October 17, 2003.

*Social Security Administration: Actions Taken to Strengthen Procedures for Issuing Social Security Numbers to Noncitizens, but Some Weaknesses Remain.* GAO-04-12. Washington, D.C.: October 15, 2003.

*Social Security Numbers: Improved SSN Verification and Exchange of States' Driver Records Would Enhance Identity Verification.* GAO-03-920. Washington, D.C.: September 15, 2003.

*H-1B Foreign Workers: Better Tracking Needed to Help Determine H-1B Program's Effects on U.S. Workforce.* GAO-03-883. Washington, D.C.: September 10, 2003.

*Supplemental Security Income: SSA Could Enhance Its Ability to Detect Residency Violations.* GAO-03-724. Washington, D.C.: July 29, 2003.

*Immigration Benefits: Ninth Report Required by the Haitian Refugee Immigration Fairness Act of 1998.* GAO-03-681R. Washington, D.C.: April 21, 2003.

## Aviation Security

*Aviation Security: Efforts to Strengthen International Passenger Prescreening Are Under Way, but Planning and Implementation Issues Remain.* GAO-07-346. Washington, D.C.: May 16, 2007.

*Aviation Security: Federal Efforts to Secure U.S.-Bound Air Cargo Are in the Early Stages and Could Be Strengthened.* GAO-07-660. Washington, D.C.: April 30, 2007.

*Aviation Security: TSA's Change to Its Prohibited Items List Has Not Resulted in Any Reported Security Incidents, but the Impact of the Change on Screening Operations Is Inconclusive.* GAO-07-634R. Washington, D.C.: April 25, 2007.

*Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved.* GAO-07-634. Washington, D.C.: April 16, 2007.

*Aviation Security: Cost Estimates Related to TSA Funding of Checked Baggage Screening Systems at Los Angeles and Ontario Airports.* GAO-07-445. Washington, D.C.: March 30, 2007.

*Aviation Security: TSA's Staffing Allocation Model Is Useful for Allocating Staff among Airports, but Its Assumptions Should Be Systematically Reassessed.* GAO-07-299. Washington, D.C.: February 28, 2007.

*Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains.* GAO-07-448T. Washington, D.C.: February 13, 2007.

*Transportation Security Administration: Oversight of Explosive Detection Systems Maintenance Contracts Can Be Strengthened.* GAO-06-795. Washington D.C.: July 31, 2006.

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

*Aviation Security: TSA Has Strengthened Efforts to Plan for the Optimal Deployment of Checked Baggage Screening Systems, but Funding Uncertainties Remain.* GAO-06-875T. Washington, D.C.: June 29, 2006.

*Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program.* GAO-06-864T. Washington, D.C.: June 14, 2006.

*Aviation Security: Further Study of Safety and Effectiveness and Better Management Controls Needed if Air Carriers Resume Interest in Deploying Less-than-Lethal Weapons.* GAO-06-475. Washington, D.C.: May 26, 2006.

*Aviation Security: Transportation Security Administration Has Made Progress in Managing a Federal Workforce and Ensuring Security at U.S. Airports, but Challenges Remain.* GAO-06-597T. Washington, D.C.: April 4, 2006.

*Aviation Security: Enhancements Made in Passenger and Checked Baggage Screening, but Challenges Remain.* GAO-06-371T. Washington, D.C.: April 4, 2006.

*Aviation Security: Progress Made to Set Up Program Using Private-Sector Airport Screeners, but More Work Remains.* GAO-06-166. Washington, D. C.: March 31, 2006.

*Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program.* GAO-06-374T. Washington, D.C.: February 9, 2006.

*Aviation Security: Federal Air Marshal Service Could Benefit from Improved Planning and Controls.* GAO-06-203. Washington, D.C.: November 28, 2005.

*Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security.* GAO-06-76. Washington, D.C.: October 17, 2005.

*Transportation Security Administration: More Clarity on the Authority of Federal Security Directors Is Needed.* GAO-05-935. Washington, D.C.: September 23, 2005.

*Aviation Security: Flight and Cabin Crew Member Security Training Strengthened, but Better Planning and Internal Controls Needed.* GAO-05-781. Washington, D.C.: September 6, 2005.

*Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing Initial Privacy Notes, but Has Recently Taken Steps to More Fully Inform the Public.* GAO-05-864R. Washington, D.C.: July 22, 2005.

*Aviation Security: Better Planning Needed to Optimize Deployment of Checked Baggage Screening Systems.* GAO-05-896T. Washington, D.C.: July 13, 2005.

*Aviation Security: Screener Training and Performance Measurement Strengthened, but More Work Remains.* GAO-05-457. Washington, D.C.: May 2, 2005.

*Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed.* GAO-05-356. Washington, D.C.: March 28, 2005.

*Aviation Security: Systematic Planning Needed to Optimize the Deployment of Checked Baggage Screening Systems.* GAO-05-365. Washington, D.C.: March 15, 2005.

*Aviation Security: Measures for Testing the Impact of Using Commercial Data for the Secure Flight Program.* GAO-05-324. Washington, D.C.: February 23, 2005.

*Transportation Security: Systematic Planning Needed to Prioritize Resources.* GAO-05-357T. Washington, D.C.: February 15, 2005.

*Aviation Security: Preliminary Observations on TSA's Progress to Allow Airports to Use Private Passenger and Baggage Screening.* GAO-05-126. Washington, D.C.: November 19, 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. Washington, D.C.: November 10, 2004.

*Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls.* GAO-04-728. Washington, D.C.: June 4, 2004.

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

*Aviation Security: Private Security Screening Contractors Have Little Flexibility to Implement Innovative Approaches.* GAO-04-505T. Washington, D.C.: April 22, 2004.

*Aviation Security: Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System.* GAO-04-504T. Washington, D.C.: March 17, 2004.

*Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges.* GAO-04-385. Washington, D.C.: February 13, 2004.

*Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges.* GAO-04-385. Washington, D.C.: February 12, 2004.

*Aviation Security: Challenges Exist in Stabilizing and Enhancing Passenger and Baggage Screening Operations.* GAO-04-440T. Washington, D.C.: February 12, 2004.

*Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs.* GAO-04-285T. Washington, D.C.: November 20, 2003.

*Aviation Security: Federal Air Marshal Service Is Addressing Challenges of Its Expanded Mission and Workforce, but Additional Actions Needed.* GAO-04-242. Washington, D. C.: November 19, 2003.

*Aviation Security: Efforts to Measure Effectiveness and Address Challenges.* GAO-04-232T. Washington, D.C.: November 5, 2003.

*Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining.* GAO-03-1173. Washington, D.C.: September 24, 2003.

*Aviation Security: Progress since September 11, 2001, and the Challenges Ahead.* GAO-03-1154T. Washington, D.C.: September 9, 2003.

*Transportation Security: Federal Action Needed to Address Security Challenges.* GAO-03-843. Washington, D.C.: June 30, 2003.

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

## Surface Transportation Security

*Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts.* GAO-07-583T. Washington, D.C.: March 7, 2007.

*Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts.* GAO-07-459T. Washington, D.C.: February 13, 2007.

*Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts.* GAO-07-442T. Washington, D.C.: February 6, 2007.

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

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

*Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts.* GAO-06-181T. Washington, D.C.: October 20, 2005.

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

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

*Transportation Security R&D: TSA and DHS Are Researching and Developing Technologies, but Need to Improve R&D Management.* GAO-04-890. Washington, D.C.: September 30, 2004.

*Surface Transportation: Many Factors Affect Investment Decisions.* GAO-04-744. Washington, D.C.: June 30, 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.

*Transportation Security: Federal Action Needed to Enhance Security Efforts.* GAO-03-1154T. Washington, D.C.: September 9, 2003.

*Transportation Security: Federal Action Needed to Help Address Security Challenges.* GAO-03-843. Washington, D.C.: June 30, 2003.

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

*Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed.* GAO-03-435. Washington, D.C.: April 30, 2003.

*Transportation Security: Post-September 11th Initiatives and Long-Term Challenges.* GAO-03-616T. New York City: April 1, 2003.

## Maritime Security

*Information on Port Security in the Caribbean Basin.* GAO-07-804R. Washington, D.C.: June 29, 2007.

*Maritime Security: Observations on Selected Aspects of the SAFE Port Act.* GAO-07-754T. Washington, D.C.: April 26, 2007.

*Transportation Security: TSA Has Made Progress in Implementing the Transportation Worker Identification Credential Program, but Challenges Remain.* GAO-07-681T. Washington, D.C.: April 12, 2007.

*Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery.* GAO-07-412. Washington, D.C.: March 28, 2007.

*Maritime Security: Public Safety Consequences of a Liquefied Natural Gas Spill Need Clarification.* GAO-07-633T. Washington, D.C.: March 21, 2007.

*Combating Nuclear Smuggling: DHS's Decision to Procure and Deploy the Next Generation of Radiation Detection Equipment Is Not Supported by Its Cost-Benefit Analysis.* GAO-07-581T. Washington, D.C.: March 14, 2007.

*Combating Nuclear Smuggling: DNDO Has Not Yet Collected Most of the National Laboratories' Test Results on Radiation Portal Monitors in Support of DNDO's Testing and Development Program.* GAO-07-347R. Washington, D.C.: March 9, 2007.

*Maritime Security: Public Safety Consequences of a Terrorist Attack on a Tanker Carrying Liquefied Natural Gas Need Clarification.* GAO-07-316. Washington, D.C.: February 22, 2007.

*Combating Nuclear Smuggling: DHS's Cost-Benefit Analysis to Support the Purchase of New Radiation Detection Portal Monitors Was Not Based on Available Performance Data and Did Not Fully Evaluate All the Monitors' Costs and Benefits*. GAO-07-133R. Washington, D.C.: October 17, 2006.

*Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*. GAO-06-982. Washington, D.C.: September 29, 2006.

*Maritime Security: Information sharing Efforts Are Improving*. GAO-06-933T. Washington, D.C.: July 10, 2006.

*Coast Guard: Observations on Agency Performance, Operations and Future Challenges*. GAO-06-448T. Washington, D.C.: June 15, 2006.

*Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System*. GAO-06-591T. Washington, D.C.: March 30, 2006.

*Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports-of-Entry, but Concerns Remain*. GAO-06-389. Washington, D.C.: March 22, 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.

*Homeland Security: Key Cargo Security Programs Can Be Improved*. GAO-05-466T. Washington, D.C.: May 26, 2005.

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

*Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts*. GAO-05-557. Washington, D.C.: April 26, 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.

*Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security.* GAO-05-404. Washington, D.C.: March 11, 2005.

*Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention.* GAO-05-170. Washington, D.C.: January 14, 2005.

*Port Security: Better 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.

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

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

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

## Emergency Preparedness and Response

*Preliminary Information on Rebuilding Efforts in the Gulf Coast.* GAO-07-809R. Washington, D.C.: June 29, 2007.

*Emergency Management: Most School Districts Have Developed Emergency Management Plans, but Would Benefit from Additional Federal Guidance.* GAO-07-609. Washington, D.C.: June 12, 2007.

*Emergency Management: Status of School Districts' Planning and Preparedness.* GAO-07-821T. Washington, D.C.: May 17, 2007.

*Homeland Security: Observations on DHS and FEMA Efforts to Prepare for and Respond to Major and Catastrophic Disasters and Address Related Recommendations and Legislation.* GAO-07-835T. Washington, D.C: May 15, 2007.

*First Responders: Much Work Remains to Improve Communications Interoperability.* GAO-07-301. Washington, D.C.: April 2, 2007.

*Emergency Preparedness: Current Emergency Alert System Has Limitations, and Development of a New Integrated System Will Be Challenging.* GAO-07-0411. Washington, D.C.: March 30, 2007.

*Hurricanes Katrina and Rita Disaster Relief: Continued Findings of Fraud, Waste, and Abuse.* GAO-07-300. Washington, D.C.: March 15, 2007.

*Disaster Assistance: Better Planning Needed for Housing Victims of Catastrophic Disasters.* GAO-07-88. Washington, D.C.: February 28, 2007.

*Homeland Security Grants: Observations on Process DHS Used to Allocate Funds to Selected Urban Areas.* GAO-07-381R. Washington, D.C.: February 7, 2007.

*Homeland Security: Applying Risk Management Principles to Guide Federal Investments.* GAO-07-386T. Washington, D.C.: February 7, 2007.

*Budget Issues: FEMA Needs Adequate Data, Plans, and Systems to Effectively Manage Resources for Day-to-Day Operations*, GAO-07-139. Washington, D.C.: January 19, 2007.

*Transportation-Disadvantaged Populations: Actions Needed to Clarify Responsibilities and Increase Preparedness for Evacuations.* GAO-07-44. Washington, D.C.: December 22, 2006.

*Homeland Security: Assessment of the National Capital Region Strategic Plan.* GAO-06-1096T. Washington, D.C.: September 28, 2006.

*Hurricanes Katrina and Rita: Unprecedented Challenges Exposed the Individuals and Households Program to Fraud and Abuse; Actions Needed to Reduce Such Problems in the Future.* GAO-06-1013. Washington, D.C.: September 27, 2006.

*Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System.* GAO-06-618. Washington, D.C.: September 6, 2006.

*Coast Guard: Observations on the Preparation, Response, and Recovery Missions Related to Hurricane Katrina.* GAO-06-903. Washington, D.C.: July 31, 2006.

*Child Welfare: Federal Action Needed to Ensure States Have Plans to Safeguard Children in the Child Welfare System Displaced by Disasters.* GAO-06-944. Washington, D.C.: July 28, 2006.

*Disaster Preparedness: Limitations in Federal Evacuation Assistance for Health Facilities Should Be Addressed.* GAO-06-826. Washington, D.C.: July 20, 2006.

*Purchase Cards: Control Weaknesses Leave DHS Highly Vulnerable to Fraudulent, Improper, and Abusive Activity.* GAO-06-957T. Washington, D.C.: July 19, 2006.

*Individual Disaster Assistance Programs: Framework for Fraud Prevention, Detection, and Prosecution.* GAO-06-954T. Washington, D.C.: July 12, 2006.

*Expedited Assistance for Victims of Hurricanes Katrina and Rita: FEMA's Control Weaknesses Exposed the Government to Significant Fraud and Abuse.* GAO-06-655. Washington, D.C.: June 16, 2006.

*Hurricanes Katrina and Rita: Improper and Potentially Fraudulent Individual Assistance Payments Estimated to Be between $600 Million and $1.4 Billion.* GAO-06-844T. Washington, D.C.: June 14, 2006.

*Hurricanes Katrina and Rita: Coordination between FEMA and the Red Cross Should Be Improved for the 2006 Hurricane Season.* GAO-06-712. Washington, D.C.: June 8, 2006.

*U.S. Tsunami Preparedness: Federal and State Partners Collaborate to Help Communities Reduce Potential Impacts, but Significant Challenges Remain.* GAO-06-519. Washington, D.C.: June 5, 2006.

*Disaster Preparedness: Preliminary Observations on the Evacuation of Vulnerable Populations due to Hurricanes and Other Disasters.* GAO-06-790T. Washington, D.C.: May 18, 2006.

*Continuity of Operations: Selected Agencies Could Improve Planning for Use of Alternate Facilities and Telework during Disruptions.* GAO-06-713. Washington, D.C.: May 11, 2006.

*Federal Emergency Management Agency: Factors for Future Success and Issues to Consider for Organizational Placement.* GAO-06-746T. Washington, D.C.: May 9, 2006.

*Hurricane Katrina: Improving Federal Contracting Practices in Disaster Recovery Operations.* GAO-06-714T. Washington, D.C.: May 4, 2006.

*Hurricane Katrina: Planning for and Management of Federal Disaster Recovery Contracts.* GAO-06-622T. Washington, D.C.: April 10, 2006.

*Hurricane Katrina: Comprehensive Policies and Procedures Are Needed to Ensure Appropriate Use of and Accountability for International Assistance.* GAO-06-460. Washington, D.C.: April 6, 2006.

*Homeland Security: The Status of Strategic Planning in the National Capital Region.* GAO-06-559T. Washington, D.C.: March 29, 2006.

*Agency Management of Contractors Responding to Hurricanes Katrina and Rita.* GAO-06-461R. Washington, D.C.: March 15, 2006.

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

*Emergency Preparedness and Response: Some Issues and Challenges Associated with Major Emergency Incidents.* GAO-06-467T. Washington, D.C.: February 23, 2006.

*Expedited Assistance for Victims of Hurricanes Katrina and Rita: FEMA's Control Weaknesses Exposed the Government to Significant Fraud and Abuse.* GAO-06-403T. Washington, D.C.: February 13, 2006.

*Statement by Comptroller General David M. Walker on GAO's Preliminary Observations Regarding Preparedness and Response to Hurricanes Katrina and Rita.* GAO-06-365R. Washington, D.C.: February 1, 2006.

*Hurricanes Katrina and Rita: Provision of Charitable Assistance.* GAO-06-297T. Washington, D.C.: December 13, 2005.

*Hurricanes Katrina and Rita: Preliminary Observations on Contracting for Response and Recovery Efforts.* GAO-06-246T. Washington, D.C.: November 8, 2005.

*Hurricanes Katrina and Rita: Contracting for Response and Recovery Efforts.* GAO-06-235T. Washington, D.C.: November 2, 2005.

*Federal Emergency Management Agency: Oversight and Management of the National Flood Insurance Program.* GAO-06-183T. Washington, D.C. October 20, 2005.

*Federal Emergency Management Agency: Challenges Facing the National Flood Insurance Program.* GAO-06-174T. Washington, D.C.: October 18, 2005.

*Federal Emergency Management Agency: Improvements Needed to Enhance Oversight and Management of the National Flood Insurance Program.* GAO-06-119. Washington, D.C.: October 18, 2005.

*Hurricane Katrina: Providing Oversight of the Nation's Preparedness, Response, and Recovery Activities.* GAO-05-1053T. Washington, D.C.: September 28, 2005.

*Homeland Security: Managing First Responder Grants to Enhance Emergency Preparedness in the National Capital Region.* GAO-05-889T. Washington, D.C.: July 14, 2005.

*Flood Map Modernization: Federal Emergency Management Agency's Implementation of a National Strategy.* GAO-05-894T. Washington, D.C.: July 12, 2005.

*Homeland Security: DHS's Efforts to Enhance First Responders' All-Hazards Capabilities Continue to Evolve.* GAO-05-652. Washington, D.C.: July 11, 2005.

*National Flood Insurance Program: Oversight of Policy Issuance and Claims.* GAO-05-532T. Washington, D.C.: April 14, 2005.

*Homeland Security: Management of First Responder Grant Programs and Efforts to Improve Accountability Continue to Evolve.* GAO-05-530T. Washington, D.C.: April 12, 2005.

*Homeland Security: Management of First Responder Grant Programs Has Improved, but Challenges Remain.* GAO-05-121. Washington, D.C.: February 2, 2005.

*Homeland Security: Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications.* GAO-04-740. Washington, D.C.: July 20, 2004.

*Homeland Security: Management of First Responder Grants in the National Capital Region Reflects the Need for Coordinated Planning and Performance Goals.* GAO-04-433. Washington, D.C.: May 28, 2004.

*Project SAFECOM: Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration.* GAO-04-494. Washington, D.C.: April 16, 2004.

*Flood Map Modernization: Program Strategy Shows Promise, but Challenges Remain.* GAO-04-417. Washington, D.C.: March 31, 2004.

*Continuity of Operations: Improved Planning Needed to Ensure Delivery of Essential Government Services.* GAO-04-160. Washington, D.C.: February 27, 2004.

*September 11: Overview of Federal Disaster Assistance to the New York City Area.* GAO-04-72. Washington, D.C.: October 31, 2003.

*Disaster Assistance: Information on FEMA's Post 9/11 Public Assistance to the New York City Area.* GAO-03-926. Washington, D.C.: August 29, 2003.

*Flood Insurance: Challenges Facing the National Flood Insurance Program.* GAO-03-606T. Washington, D.C.: April 1, 2003.

## Critical Infrastructure and Key Resources Protection

*Information Technology: Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives.* GAO-07-822T. Washington, D.C.: May 10, 2007.

*Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information sharing Initiatives.* GAO-07-455. Washington, D.C.: April 16, 2007.

*DHS Multi-Agency Operation Centers Would Benefit from Taking Further Steps to Enhance Collaboration and Coordination.* GAO-07-686R. Washington, D.C.: April 5, 2007.

*Critical Infrastructure: Challenges Remain in Protecting Key Sectors.* GAO-07-626T. Washington, D.C.: March 20, 2007.

*Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts.* GAO-07-583T. Washington, D.C.: March 7, 2007.

*Homeland Security: Applying Risk Management Principles to Guide Federal Investments.* GAO-07-386T. Washington, D.C.: February 7, 2007.

*Homeland Security Grants: Observations on Process DHS Used to Allocate Funds to Selected Urban Areas.* GAO-07-381R. Washington, D.C.: February 7, 2007.

*Homeland Security: Opportunities Exist to Enhance Collaboration at 24/7 Operations Centers Staffed by Multiple DHS Agencies.* GAO-07-89. Washington, D.C.: October 20, 2006.

*Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics.* GAO-07-39. Washington, D.C.: October 16, 2006.

*Information Security: Coordination of Federal Cyber Security Research and Development.* GAO-06-811. Washington, D.C.: September 29, 2006.

*Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity.* GAO-06-1087T. Washington, D.C.: September 13, 2006.

*Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System.* GAO-06-618. Washington, D.C.: September 6, 2006.

*Homeland Security: DHS Is Addressing Security at Chemical Facilities, but Additional Authority Is Needed.* GAO-06-899T. Washington, D.C.: June 21, 2006.

*Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan.* GAO-06-672. Washington, D.C.: June 16, 2006.

*Homeland Security: Guidance and Standards Are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts.* GAO-06-612. Washington, D.C: May 31, 2006.

*Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information.* GAO-06-383. Washington, D.C.: April 17, 2006.

*Securing Wastewater Facilities: Utilities Have Made Important Upgrades but Further Improvements to Key System Components May Be Limited by Costs and Other Constraints.* GAO-06-390. Washington, D.C.: March 31, 2006.

*Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information.* GAO-06-385. Washington, D.C.: March 17, 2006.

*Homeland Security: DHS Is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority Is Needed.* GAO-06-150. Washington, D.C.: January 27, 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.

*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.

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

*Homeland Security: Much Is Being Done to Protect Agriculture from a Terrorist Attack, but Important Challenges Remain.* GAO-05-214. Washington, D.C.: March 8, 2005.

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

*Technology Assessment: Cybersecurity for Critical Infrastructure Protection.* GAO-04-321. Washington, D.C.: May 28, 2004.

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

*Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems.* GAO-04-628T. Washington, D.C.: March 30, 2004.

*Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems.* GAO-04-354. Washington, D.C.: March 15, 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.

*Drinking Water: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security.* GAO-04-29. Washington, D.C.: October 31, 2003.

*Critical Infrastructure Protection: Challenges in Securing Control Systems.* GAO-04-140T. Washington, D.C.: October 1, 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: 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.

## Science and Technology

*Department of Homeland Security: Science and Technology Directorate's Expenditure Plan.* GAO-07-868. Washington, D.C.: June 22, 2007.

*Combating Nuclear Smuggling: DHS's Decision to Procure and Deploy the Next Generation of Detection Equipment Is Not Supported by Its Cost-Benefit Analysis.* GAO-07-581T. Washington, D.C.: March 14, 2007.

*Combating Nuclear Smuggling: DNDO Has Not Yet Collected Most of the National Laboratories' Test Results on Radiation Portal Monitors in Support of DNDO's Testing and Development Program.* GAO-07-347R. Washington, D.C.: March 9, 2007.

*Homeland Security: DHS Needs to Improve Ethics-Related Management Controls for the Science and Technology Directorate.* GAO-06-206. Washington, D.C.: December 22, 2006.

*Combating Nuclear Smuggling: DHS's Cost-Benefit Analysis to Support the Purchase of New Radiation Detection Portal Monitors Was Not Based on Available Performance Data and Did Not Fully Evaluate All the Monitors' Costs and Benefits.* GAO-07-133R. Washington, D.C.: October 17, 2006.

*Combating Nuclear Terrorism: Federal Efforts to Respond to Nuclear and Radiological Threats and to Protect Emergency Response Capabilities Could Be Strengthened.* GAO-06-1015. Washington, D.C.: September 21, 2006.

*Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports-of-Entry, but Concerns Remain.* GAO-06-389. Washington, D.C.: March 22, 2006.

*Combating Nuclear Smuggling: Corruption, Maintenance, and Coordination Problem Challenge U.S. Effort to Provide Radiation*

*Detection Equipment to Other Countries.* GAO-06-311. Washington, D.C.: March 14, 2006.

*Transportation Security R&D: TSA and DHS Are Researching and Developing Technologies, but Need to Improve R&D Management.* GAO-04-890. Washington, D.C.: September 30, 2004.

*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 24, 2004.

## Acquisition Management

*Coast Guard: Challenges Affecting Deepwater Asset Deployment and Management and Efforts to Address Them.* GAO-07-874. Washington, D.C.: June 18, 2007.

*Department of Homeland Security: Progress and Challenges in Implementing the Department's Acquisition Oversight Plan.* GAO-07-900. Washington, D.C.: June 13, 2007.

*Department of Homeland Security: Ongoing Challenges in Creating an Effective Acquisition Organization.* GAO-07-948T. Washington, D.C.: June 7, 2007.

*Homeland Security: Observations on the Department of Homeland Security's Acquisition Organization and on the Coast Guard's Deepwater Program.* GAO-07-453T. Washington, D.C.: February 8, 2007.

*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.

*Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System.* GAO-06-618. Washington, D.C.: September 6, 2006.

*Homeland Security: Challenges in Creating an Effective Acquisition Organization.* GAO-06-1012T. Washington, D.C.: July 27, 2006.

*Coast Guard: Status of Deepwater Fast Response Cutter Design Efforts.* GAO-06-764. Washington, D.C.: June 23, 2006.

*Coast Guard: Changes to Deepwater Appear Sound, and Program Management Has Improved, But Continued Monitoring Is Warranted.* GAO-06-546. Washington, D.C.: April 28, 2006.

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

*Homeland Security: Successes and Challenges in DHS's Efforts to Create an Effective Acquisition Organization.* GAO-05-179. Washington, D.C.: March 29, 2005.

*Homeland Security: Further Action Needed to Promote Successful Use of Special DHS Acquisition Authority.* GAO-05-136. Washington, D.C.: December 15, 2004.

*Coast Guard: Deepwater Program Acquisition Schedule Update Needed.* GAO-04-695. Washington, D.C.: June 14, 2004.

*Contract Management: Coast Guard's Deepwater Program Needs Increased Attention to Management and Contractor Oversight.* GAO-04-380. Washington, D.C.: March 9, 2004.

*Contract Management: INS Contracting Weaknesses Need Attention from the Department of Homeland Security.* GAO-03-799. Washington, D.C.: July 25, 2003.

## Financial Management

*Purchase Cards: Control Weaknesses Leave DHS Highly Vulnerable to Fraudulent, Improper, and Abusive Activity.* GAO-06-1117. Washington, D.C.: September 28, 2006.

*Internal Control: Analysis of Joint Study on Estimating the Costs and Benefits of Rendering Opinions on Internal Control over Financial Reporting in the Federal Environment.* GAO-06-255R. Washington, D.C.: September 6, 2006.

*Financial Management: Challenges Continue in Meeting Requirements of the Improper Payments Information Act.* GAO-06-581T. Washington, D.C.: April 5, 2006.

*Financial Management Systems: DHS Has an Opportunity to Incorporate Best Practices in Modernization Efforts.* GAO-06-553T. Washington, D.C.: March 29, 2006.

*Financial Management Systems: Additional Efforts Needed to Address Key Causes of Modernization Failures.* GAO-06-184. Washington, D.C.: March 15, 2006.

*Financial Management: Challenges Remain in Meeting Requirements of the Improper Payments Information Act.* GAO-06-482T. Washington, D.C.: March 9, 2006.

*CFO Act of 1990: Driving the Transformation of Federal Financial Management.* GAO-06-242T. Washington, D.C.: November 17, 2005.

*Financial Management: Achieving FFMIA Compliance Continues to Challenge Agencies.* GAO-05-881. Washington, D.C.: September 20, 2005.

*Financial Audit: The Department of Homeland Security's Fiscal Year 2004 Management Representation Letter on Its Financial Statements.* GAO-05-600R. Washington, D.C.: July 14, 2005.

*Financial Management: Challenges in Meeting Requirements of the Improper Payments Information Act.* GAO-05-417. Washington, D.C.: March 31, 2005.

*Financial Management: Effective Internal Control Is Key to Accountability.* GAO-05-321T. Washington, D.C.: February 16, 2005.

*Financial Management: Improved Financial Systems Are Key to FFMIA Compliance.* GAO-05-20. Washington, D.C.: October 1, 2004

*Financial Management: Department of Homeland Security Faces Significant Financial Management Challenges.* GAO-04-774. Washington, D.C.: July 19, 2004.

*Department of Homeland Security: Financial Management Challenges.* GAO-04-945T. Washington, D.C.: July 8, 2004.

*Financial Management: Recurring Financial Systems Problems Hinder FFMIA Compliance.* GAO-04-209T. Washington, D.C.: October 29, 2003

*Department of Homeland Security: Challenges and Steps in Establishing Sound Financial Management.* GAO-03-1134T. Washington, D.C.: September 10, 2003.

## Human Capital Management

*Homeland Security: Management and Programmatic Challenges Facing the Department of Homeland Security.* GAO-07-833T. Washington, D.C.: May 10, 2007.

*Homeland Security: Information on Training New Border Patrol Agents.* GAO-07-540R. Washington, D.C.: March 30, 2007.

*Homeland Security: Management and Programmatic Challenges Facing the Department of Homeland Security.* GAO-07-452T. Washington, D.C.: February 7, 2007.

*Budget Issues: FEMA Needs Adequate Data, Plans, and Systems to Effectively Manage Resources for Day-to-Day Operations.* GAO-07-139. Washington, D.C.: January 19, 2007.

*Department of Homeland Security: Strategic Management of Training Important for Successful Transformation.* GAO-05-888. Washington, D.C.: September 23, 2005.

*Human Capital: Observations on Final DHS Human Capital Regulations.* GAO-05-391T. Washington, D.C.: March 2, 2005.

*Human Capital: DHS Faces Challenges In Implementing Its New Personnel System.* GAO-04-790. Washington, D.C.: June 18, 2004.

*Human Capital: DHS Personnel System Design Effort Provides for Collaboration and Employee Participation.* GAO-03-1099. Washington, D.C.: September 30, 2003.

## Information Technology Management

*Homeland Security: DHS Enterprise Architecture Continues to Evolve but Improvements Needed.* GAO-07-564. Washington, D.C.: May 9, 2007.

*Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments.* GAO-07-424. Washington, D.C.: April 27, 2007.

*Homeland Security: Planned Expenditures for U.S. Visitor and Immigrant Status Program Need to Be Adequately Defined and Justified.* GAO-07-278. Washington, D.C.: February 14, 2007.

*Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation.* GAO-06-831. Washington, D.C.: August 14, 2006.

*Information Technology: Immigration and Customs Enforcement Is Beginning to Address Infrastructure Modernization Program Weaknesses, but Key Improvements Still Needed.* GAO-06-823. Washington, D.C.: July 27, 2006.

*Information Technology: Customs Has Made Progress on Automated Commercial Environment System, but It Faces Long-Standing Management Challenges and New Risks.* GAO-06-580. Washington, D.C.: May 31, 2006.

*Homeland Security Progress Continues but Challenges Remain on Department's Management of Information Technology.* GAO-06-598T. Washington, D.C.: March 29, 2006.

*Information Technology: Management Improvements Needed on Immigration and Customs Enforcement's Infrastructure Modernization Program.* GAO-05-805. Washington, D.C.: September 7, 2005.

*Information Security: Department of Homeland Security Needs to Fully Implement Its Security Program.* GAO-05-700. Washington, D.C: June 17, 2005.

*Information Security: Department of Homeland Security Faces Challenges in Fulfilling Statutory Requirements.* GAO-05-567T. Washington, D.C.: April 14, 2005.

*Information Technology: Customs Automated Commercial Environment Program Progressing, but Need for Management Improvements Continues.* GAO-05-267. Washington, D.C.: March 14, 2005.

*Homeland Security: Some Progress Made, but Many Challenges Remain on U.S. Visitor and Immigrant Status Indicator Technology Program.* GAO-05-202. Washington, D.C.: February 23, 2005.

*Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach.* GAO-04-702. Washington, D.C.: August 27, 2004.

*Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains.* GAO-04-777. Washington, D.C.: August 6, 2004.

*Information Technology: Homeland Security Should Better Balance Need for System Integration Strategy with Spending for New and Enhanced Systems.* GAO-04-509. Washington, D.C.: May 21, 2004.

*Information Technology: Early Releases of Customs Trade System Operating, but Pattern of Cost and Schedule Problems Needs to Be Addressed.* GAO-04-719. Washington, D.C.: May 14, 2004.

*Information Technology: OMB and Department of Homeland Security Investment Reviews.* GAO-04-323. Washington, D.C.: February 10, 2004.

*Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed.* GAO-03-1083. Washington, D.C.: September 19, 2003.

*Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1).* GAO-03-584G. Washington, D.C.: April 2003.

## Real Property Management

*Federal Real Property: DHS Has Made Progress, but Additional Actions Are Needed to Address Real Property Management and Security Challenges.* GAO-07-658. Washington, D.C.: June 22, 2007.

## General Reports

*Homeland Security: Guidance from Operations Directorate Will Enhance Collaboration among Departmental Operations Centers.* GAO-07-683T. Washington, D.C.: June 20, 2007.

*Homeland Security: Management and Programmatic Challenges Facing the Department of Homeland Security.* GAO-07-833T. Washington, D.C.: May 10, 2007.

*DHS Privacy Office: Progress Made but Challenges Remain in Notifying and Reporting to the Public.* GAO-07-522. Washington, D.C.: April 27, 2007.

*Transportation Security: DHS Efforts to Eliminate Redundant Background Check Investigations*, GAO-07-756. Washington, D.C.: April 26, 2007.

*Department of Homeland Security: Observations on GAO Access to Information on Programs and Activities.* GAO-07-700T. Washington, D.C.: April 25, 2007.

*DHS Multi-Agency Operation Centers Would Benefit from Taking Further Steps to Enhance Collaboration and Coordination.* GAO-07-686R. Washington, D.C.: April 5, 2007.

*Homeland Security: Applying Risk Management Principles to Guide Federal Investments.* GAO-07-386T. Washington, D.C.: February 7, 2007.

*Homeland Security: Management and Programmatic Challenges Facing the Department of Homeland Security.* GAO-07-452T. Washington, D.C.: February 7, 2007.

*Homeland Security: Management and Programmatic Challenges Facing the Department of Homeland Security.* GAO-07-398T. Washington, D.C.: February 6, 2007.

*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.

*Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public.* GAO-06-1031. Washington, D.C.: September 29, 2006.

*Combating Terrorism: Determining and Reporting Federal Funding Data.* GAO-06-161. Washington, D.C.; January 17, 2006.

*Homeland Security: Overview of Department of Homeland Security Management Challenges.* GAO-05-573T. Washington, D.C.: April 20, 2005.

*Results-Oriented Government: Improvements to DHS's Planning Process Would Enhance Usefulness and Accountability.* GAO-05-300. Washington, D.C.: March 31, 2005.

*September 11: Recent Estimates of Fiscal Impact of 2001 Terrorist Attack on New York.* GAO-05-269. Washington, D.C.; March 30, 2005.

*Department of Homeland Security: A Comprehensive and Sustained Approach Needed to Achieve Management Integration.* GAO-05-139. Washington, D.C.; March 16, 2005.

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

*Homeland Security: Effective Regional Coordination Can Enhance Emergency Preparedness.* GAO-04-1009. Washington, D.C.: September 15, 2004.

*Intelligence Reform: Human Capital Considerations Critical to 9/11 Commission's Proposed Reforms.* GAO-04-1084T. Washington, D.C.: September 14, 2004.

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

*The Chief Operating Officer Concept and its Potential Use as a Strategy to Improve Management at the Department of Homeland Security.* GAO-04-876R. Washington, D.C.: June 28, 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.

*Transfer of Budgetary Resources to the Department of Homeland Security (DHS).* GAO-04-329R. Washington, D.C.: April 30, 2004.

*Homeland Security: Selected Recommendations from Congressionally Chartered Commissions and GAO.* GAO-04-591. Washington, D.C.: March 31, 2004.

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

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

## 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

Susan Becker, Acting Manager, Beckers@GAO.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER