United States Government Accountability Office

GAO

Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

January 2005

# HOMELAND SECURITY

# Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security


GAO-05-33

January 2005

# HOMELAND SECURITY

# Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security

GAO Highlights

Highlights of GAO-05-33, a report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

## Why GAO Did This Study

The *National Strategy for Homeland Security* sets forth a plan to improve homeland security through the cooperation of federal, state, local, and private sector organizations on an array of functions. These functions are organized into the six distinct "critical mission areas" of (1) intelligence and warning, (2) border and transportation security, (3) domestic counterterrorism, (4) protecting critical infrastructures and key assets, (5) defending against catastrophic threats, and (6) emergency preparedness and response. Within each of these mission areas, the strategy identifies "major initiatives" to be addressed. In all, the strategy cites 43 initiatives across the six mission areas.

GAO reviewed the strategy's implementation to

- determine whether its initiatives are being addressed by key departments' strategic planning and implementation activities, whether the initiatives have lead agencies identified for their implementation, and whether the initiatives were being implemented in fiscal year 2004 by such agencies and
- identify ongoing homeland security challenges that have been reflected in GAO products since September 11, 2001, by both mission area and issues that cut across mission areas.

www.gao.gov/cgi-bin/getrpt?GAO-05-33.

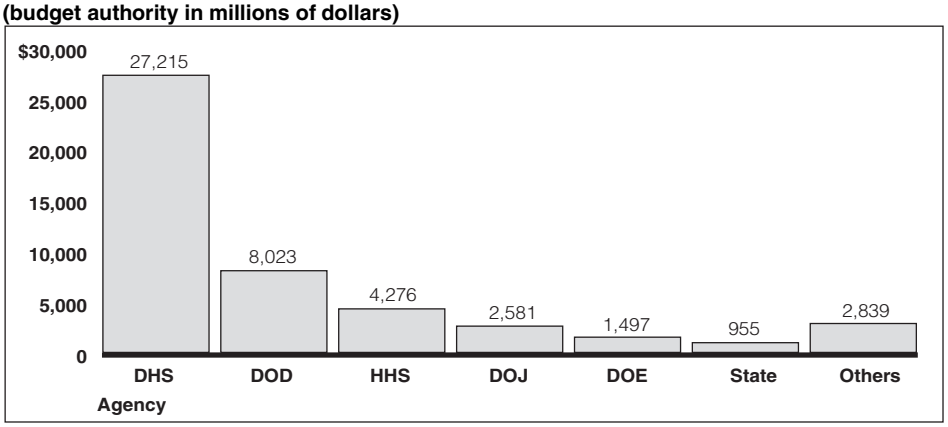
To view the full product, including the scope and methodology, click on the link above. For more information, contact Norman J. Rabkin (202) 512-3610 or rabkinn@gao.gov.

## What GAO Found

Key federal departments—Defense (DOD), Energy (DOE), Health and Human Services (HHS), Homeland Security (DHS), Justice (DOJ), and State—have addressed the strategy's 43 initiatives to some extent in their strategic planning and implementation activities. All 43 of the initiatives were included in some of the planning or implementation activities of at least one of these six departments. Most of the initiatives (42 of the 43) also had departments identified as the lead agencies for their implementation, which helps to ensure accountability for implementation. However, many of these 42 initiatives had multiple lead agencies, indicating that interagency coordination of roles and activities will be important, particularly on those initiatives involving domestic counterterrorism and critical infrastructure protection. All of the initiatives were being implemented in fiscal year 2004 by at least one department. While GAO determined that implementation was occurring, it did not assess the status or quality of the various departments' implementation of the initiatives.

While departments have incorporated these initiatives into their planning and implementation activity, the United States faces significant challenges in fully implementing the strategy in a coordinated and integrated manner. Some of the most difficult challenges being confronted are those that cut across the various critical mission areas, such as balancing homeland security funding needs with other national requirements, improving risk management methods for resource allocation and investments, developing adequate homeland security performance measures, developing a national enterprise architecture for homeland security, and clarifying the roles and responsibilities among the levels of government and the private sector. GAO has also identified a large diversity of other challenges in each of the six critical mission areas since September 11.

**Proposed Fiscal Year 2005 Homeland Security Funding by Agency (budget authority in millions of dollars)**




Source: Office of Management and Budget.

# Contents

## Tables

## Figures

**Abbreviations**

| | |
|---|---|
| APHIS | Animal and Plant Health Inspection Service |
| ATSA | Aviation and Transportation Security Act |
| CAPPS | Computer-Assisted Passenger Prescreening Program |
| CBP | Customs and Border Patrol |
| CBRN | chemical, biological, radiological, or nuclear |
| CIA | Central Intelligence Agency |
| CIP | Critical Infrastructure Protection |
| CSI | container security initiative |
| C-TPAT | Customs-Trade Partnership against Terrorism |
| CWC | Chemical Weapons Convention |
| DBT | design basis threat |
| DHS | Department of Homeland Security |
| DIA | Defense Intelligence Agency |
| DOD | Department of Defense |
| DOE | Department of Energy |
| DOJ | Department of Justice |
| EPA | Environmental Protection Agency |
| FBI | Federal Bureau of Investigation |
| FPS | Federal Protective Service |
| GAO | Government Accountability Office |
| GPRA | Government Performance and Results Act |
| GSA | General Services Administration |

| | |
|---|---|
| HHS | Department of Health and Human Services |
| HSAS | Homeland Security Advisory System |
| HSC | Homeland Security Council |
| HSPD | Homeland Security Presidential Directive |
| IAIP | Information Analysis and Infrastructure Protection |
| ICE | Immigration and Customs Enforcement |
| IT | information technology |
| MANPADS | Man-Portable Air Defense System |
| MTSA | Maritime Transportation Security Act |
| NIH | National Institutes of Health |
| NCR | National Capital Region |
| NMLS | National Money Laundering Strategy |
| NNSA | National Nuclear Security Administration |
| NRC | Nuclear Regulatory Commission |
| NSPD | National Security Presidential Directive |
| ODP | Office of Domestic Preparedness |
| OJP | Office of Justice Programs |
| OMB | Office of Management and Budget |
| PDD | Presidential Decision Directive |
| PSV | post-shipment verification |
| UAV | unmanned aerial vehicle |
| USDA | United States Department of Agriculture |
| USPS | United States Postal Service |
| US-VISIT | United States Visitor and Immigrant Status Indicator |
| VA | Veterans Administration |
| WMD | weapons of mass destruction |
| SSN | Social Security Number |
| TSA | Transportation Security Act |
| TTIC | Terrorist Threat Integration Center |

GAO
Accountability * Integrity * Reliability

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

January 14, 2005

The Honorable Christopher Shays
Chairman, Subcommittee on National Security, Emerging
Threats, and International Relations
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

In an effort to increase homeland security following the September 11, 2001, terrorist attacks on the United States, President Bush issued the *National Strategy for Homeland Security* in July 2002 and signed legislation creating the Department of Homeland Security (DHS) in November 2002.[1] The strategy sets 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. To accomplish these overall objectives, the strategy describes six critical mission areas and 43 initiatives. Since the strategy was issued, the President has also issued additional documents—known as Homeland Security Presidential Directives (or HSPDs)—that provide more detailed guidance on the mission areas and initiatives. The creation of DHS, which began operations in March 2003, represents a fusion of 22 federal agencies to coordinate and centralize the leadership of many homeland security activities under a single department. In addition to DHS, the Departments of Defense (DOD), Energy (DOE), Health and Human Services (HHS), Justice (DOJ), and State play an important role in implementing the strategy. These six key departments represent 94 percent of proposed federal spending for homeland security in fiscal year 2005.

With the strategy now more than 2 years old, and DHS more than a year old, you asked that we review the implementation of the strategy and organize our work by critical mission area. In response, we have

- determined whether the initiatives in the strategy were being addressed by the key department's strategic planning and related activities;

[1] *Homeland Security Act of 2002*, Pub.L. 107-296 (Nov. 25, 2002).

whether the initiatives had "lead" agencies identified for their implementation, and whether multiple departments were implementing the initiatives in fiscal year 2004; and

- identified homeland security challenges as reflected in our products since September 11, 2001, by both mission area and issues that cut across mission areas.

This report establishes one framework from which to assess federal department implementation of the *National Strategy for Homeland Security*. Since agency homeland security activities are ongoing, this report is intended to identify a baseline from which to assess progress toward meeting homeland security objectives. In this report, we first provide the proposed fiscal year 2005 homeland security-related budget by mission area and department. Then, we discuss the homeland security planning and implementation activities of the six departments under review, as well as remaining homeland security challenges, by mission area. The appendixes that follow provide more detailed assessments of each of these sections and are also arranged by mission area. (See app. I for more information on the scope and methodology.) Further, this report should be considered in the context of several companion efforts to provide baseline information. In February 2004, we testified on the desired characteristics of national strategies and whether various strategies—including the *National Strategy for Homeland Security*—contained those desired characteristics.[2] In March, we summarized strategic homeland security recommendations made by congressionally chartered commissions and us.[3] We organized this analysis by critical mission area, as defined in the strategy. In July, we reported on our recommendations to DHS and the department's progress in implementing such recommendations.[4] We organized this analysis by DHS directorate or division. In September, we compared 9/11 Commission recommendations with those of the *National Strategy for Homeland Security* and the *National Strategy to Combat Terrorism*. We also provided a preliminary analysis of department planning and implementation activities with

[2]See GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[3]See GAO, *Homeland Security: Selected Recommendations from Congressionally Chartered Commissions and GAO*, GAO-04-591 (Washington, D.C.: Mar. 31, 2004).

[4]See GAO, *Status of Key Recommendations GAO Has Made to DHS and Its Legacy Agencies*, GAO-04-865R (Washington, D.C.: July 2, 2004).

respect to the six mission areas.[5] Together, these baseline efforts are intended to aid congressional oversight of federal homeland security activities.

## Results in Brief

Key federal departments have addressed the strategy's initiatives in their strategic planning and implementation activities. All 43 initiatives indicated in the strategy were included in the activities of at least one of the six departments we reviewed. For most of the initiatives (42 of 43), the strategy or HSPDs identified lead agencies, thereby helping to ensure accountability for implementation. All 43 initiatives were being implemented in fiscal year 2004 by at least one department. Thirty-three of the 43 initiatives (77 percent) were being planned or implemented by 3 or more departments. While we determined that implementation was occurring, we did not assess the status or quality of the various departments' implementation of the initiatives.

While departments have incorporated these initiatives into their planning and implementation activity, the United States still faces significant challenges in implementing the strategy in a well coordinated and integrated manner. A review of our products since September 11, 2001, shows that some of the most difficult challenges being confronted are those that cut across the various critical mission areas. These challenges include

- balancing homeland security needs with other national requirements,
- improving risk management methods for resource allocation and investments,
- developing adequate homeland security performance measures,
- clarifying the roles and responsibilities among the levels of government and the private sector, and
- developing a national blueprint—called an enterprise architecture—to help integrate different organization's efforts to improve homeland security.

[5]See GAO, *Homeland Security: Observations on the National Strategies Related to Terrorism*, GAO-04-1075T (Washington, D.C.: Sept. 22, 2004).

In addition to these and other crosscutting challenges, we have identified a large diversity of challenges related specifically to each of the six mission areas described in the strategy and provide details on them in the remainder of the report.

We provided a draft of this report to DHS, DOD, DOE, DOJ, HHS, State, and the Homeland Security Council for comment. All except State and the Homeland Security Council provided comments, which generally consisted of technical comments that we incorporated as appropriate. None of the departments disagreed with the substance of the report.

## Background

The *National Strategy for Homeland Security* sets 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.[6] The strategy organizes these functions into six critical mission areas:[7]

- *Intelligence and Warning* involves the identification, collection, analysis, and distribution of intelligence information appropriate for preempting or preventing a terrorist attack.
- *Border and Transportation Security* emphasizes the efficient and reliable flow of people, goods, and material across borders while deterring terrorist activity.
- *Domestic Counterterrorism* focuses on law enforcement efforts to identify, halt, prevent, and prosecute terrorists in the United States.

[6]There were several other related national strategies issued subsequent to the *National Strategy for Homeland Security*. These include the *National Money Laundering Strategy*, the *National Security Strategy*, the *National Strategy to Combat Weapons of Mass Destruction*, the *National Strategy for Combating Terrorism*, the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, and the *National Strategy to Secure Cyberspace*. For our analysis of all of these strategies, see GAO-04-408T.

[7]The strategy also includes a discussion of "foundations," which we did not identify separately in our analysis. The strategy describes these foundations as unique American strengths that cut across all sectors of society, such as law, science and technology, information sharing and systems, and international cooperation. The discussion of these foundations overlaps with the six mission areas. For example, the initiative to improve international shipping security is covered by both the mission area of Border and Transportation Security as well as the foundation of international cooperation. To some extent, our discussion of crosscutting issues also acknowledges issues that cut across all sectors.

- *Protecting Critical Infrastructure and Key Assets* stresses securing the nation's interconnecting sectors and important facilities, sites, and structures.

- *Defending Against Catastrophic Threats* emphasizes the detection, deterrence, and mitigation of terrorist use of weapons of mass destruction.

- *Emergency Preparedness and Response* highlights damage minimization and recovery from terrorist attacks.

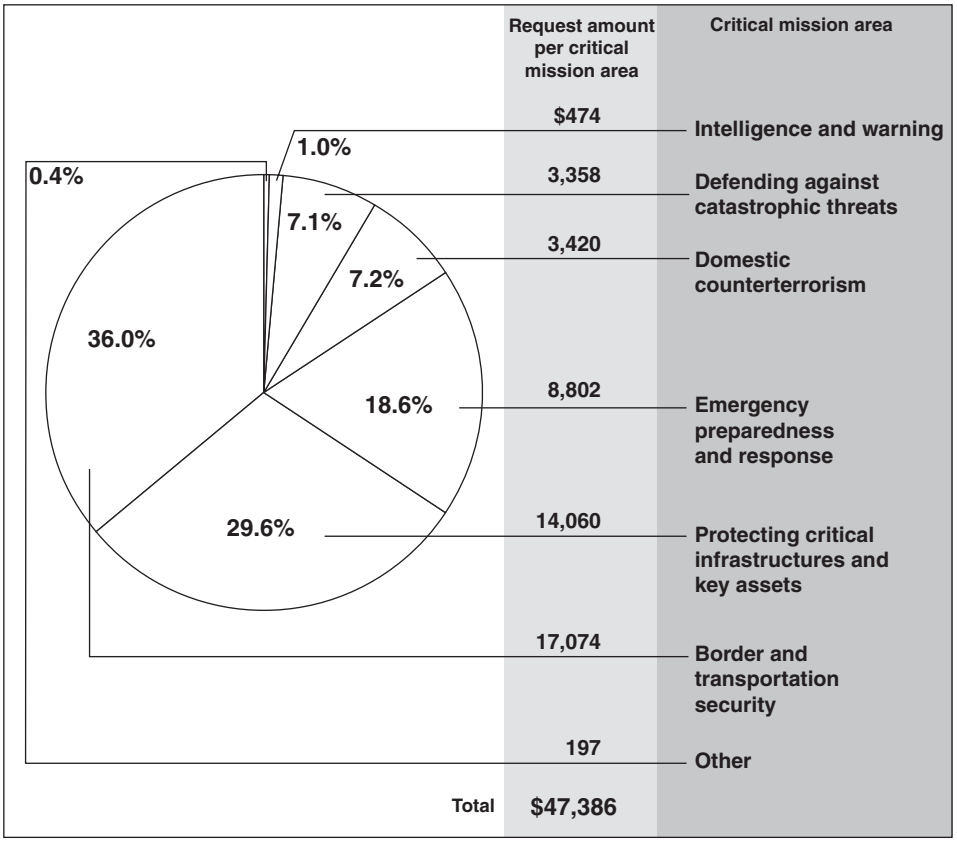
Since the strategy was issued in July 2002, the President has also issued 12 HSPDs that provide additional guidance related to these mission areas. For example, HSPD-4 focuses on defending against catastrophic threats and HSPD-7 focuses on protecting critical infrastructure. These HSPDs provided some of the details that were not in the strategy, particularly with respect to agency roles and milestones. See appendix X for a complete list and description of these HSPDs.

The strategy also identifies the major initiatives to be addressed within each of these six mission areas. For example, within the Intelligence and Warning mission area, 5 initiatives are indicated: (1) enhancing the analytic capabilities of the FBI; (2) building new capabilities through the Information Analysis and Infrastructure Protection Directorate of DHS; (3) implementing the Homeland Security Advisory System; (4) utilizing dual-use analysis to prevent attacks; and (5) employing "red team" techniques.[8] Within the Border and Transportation Security mission area, 6 initiatives are cited: (1) ensuring accountability in border and transportation security, (2) creating "smart borders", (3) increasing the security of international shipping containers, (4) implementing the Aviation and Transportation Security Act of 2001, (5) recapitalizing the U.S. Coast Guard, and (6) reforming immigration services. In all, the strategy cites 43 initiatives across the six mission areas. See appendix IX for a complete list of all the initiatives by mission area.

The latest available funding data from the Office of Management and Budget (OMB) for the six mission areas is illustrated in figure 1.

[8]Red-team techniques are those where the U.S. government would create a team that plays the role of terrorists in terms of identifying vulnerabilities and planning attacks.

**Figure 1: Proposed Fiscal Year 2005 Homeland Security Funding by Critical Mission Area**



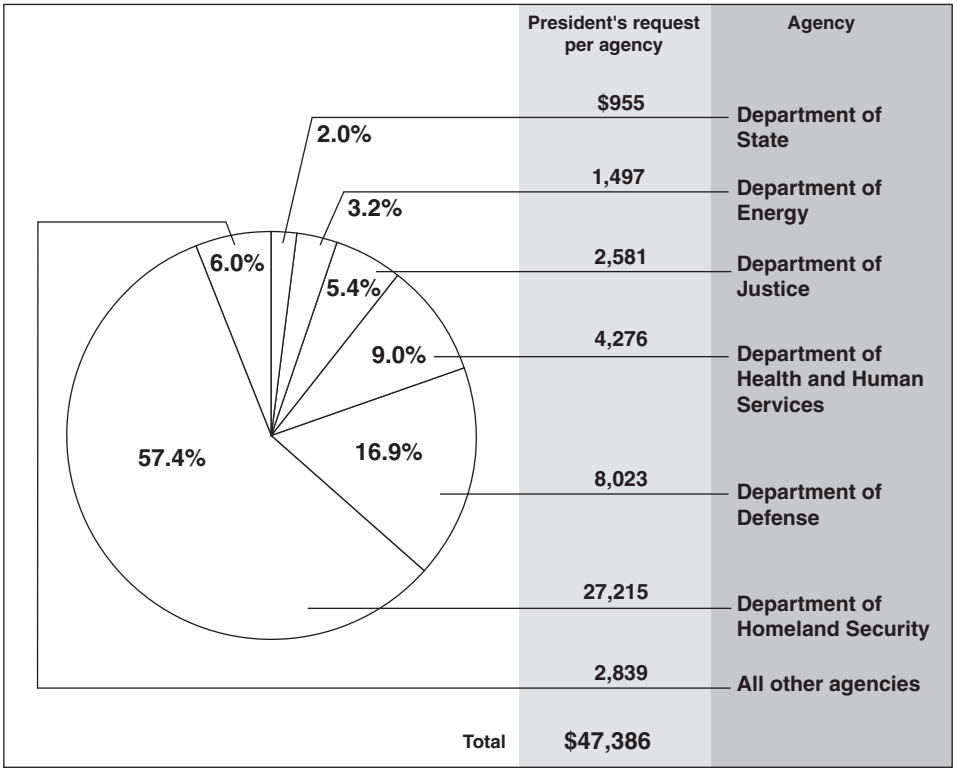

Source: GAO, based on OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005.*

Note: Budget authority in millions of dollars.

The *National Strategy for Homeland Security* specifies a number of federal departments, as well as nonfederal organizations, that have important roles in implementing the mission areas and related initiatives. In terms of federal departments, DHS is intended to have a prominent role in implementing all of the mission areas. Other key federal departments specified in the strategy include, in alphabetical order, the Department of Defense, the Department of Energy, the Department of Health and Human Services, the Department of Justice, and the Department of State (State). These departments have their own strategic plans, which indicate how they will implement their homeland security programs (as well as other programs unrelated to homeland security). Together, DHS and these other five departments constitute 94 percent of the proposed $47.4 billion

budget for homeland security-related activities in fiscal year 2005. OMB did not report funding for the Central Intelligence Agency (CIA) although it has activities related to the Intelligence and Warning mission area. As explained further in appendix II, we did not include the CIA in our analysis because of the lack of funding data and because the strategy provides little discussion of the agency. Figure 2 shows the proposed fiscal year 2005 funding for these departments as well as the proposed homeland security funding for all other agencies.

**Figure 2: Proposed Fiscal Year 2005 Homeland Security Funding by Department**




Source: GAO, based on OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005.*

Notes: Budget authority in millions of dollars.

Other agencies includes the Departments of Agriculture ($651 million), Veterans Affairs ($297 million), Transportation ($243 million), Commerce ($150 million), and Treasury ($87 million), as well as the National Science Foundation ($344 million), National Aeronautics and Space Administration ($207 million), Social Security Administration ($155 million), Environmental Protection Agency ($97 million), U.S. Army Corps of Engineers ($84 million), General Services Administration ($80 million), and several smaller agencies. Additionally, OMB reported the Intelligence Community figure in aggregate; it did not break it out by individual departments (e.g., Central Intelligence Agency).

The *National Strategy for Homeland Security* and the related HSPDs typically identify a specific federal department as being a "lead" agency for specific initiatives. However, the language varies in precision. In some cases, the documents use clear language to identify which department will lead efforts across the government. In other cases, the lead is more implied than stated. Sometimes, more than one department is identified as a lead agency—which can occur because some of the initiatives in the strategy are large in scope, and different departments lead different parts of the initiatives. The identification of lead agency is important in order to specify which agencies are accountable for the implementation of the

initiatives, particularly if implementation requires the efforts of several different agencies exercising different statutory authorities. By clearly identifying the lead agency, the strategies and the HSPDs enable the federal, state, local, and private stakeholders to determine who is responsible and accountable for the implementation, and thus more effectively direct their inquiries and integrate their own actions, particularly where multiagency coordination is required. See appendix IX for a complete list of the initiatives and the departments identified as lead agencies.

Congress, because of concerns about terrorism in recent years, chartered four commissions to examine terrorist threats and the government's response to such threats, as well as to make recommendations to federal, state, local, and private organizations. These national commissions included the following:

- *The Bremer Commission*: the National Commission on Terrorism, chaired by Ambassador Paul Bremer, which issued its report in June 2000.
- *The Gilmore Commission*: the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, chaired by Governor James S. Gilmore, III, which issued its final report in December 2003.
- *The Hart-Rudman Commission*: the U.S. Commission on National Security/21st Century, chaired by Senators Gary Hart and Warren B. Rudman, which issued its final report in February 2001.
- *The 9/11 Commission*: the National Commission on Terrorist Attacks upon the United States, chaired by Governor Thomas H. Kean, which issued its final report in July 2004.

## Scope and Methodology

To determine whether the key federal departments addressed strategy initiatives in their planning and implementation activity, we identified the 43 major initiatives and the six key federal departments for review. We evaluated each department's high-level strategic planning documents related to homeland security to determine if they had planning or implementation activities related to each initiative. To satisfy the planning and implementation criteria, we generally required departments to provide documentary support for one such activity, per initiative. Where classified or undocumented activities were involved, we worked with department officials to verify the activity. We provided the results of our analyses to

planning officials from the various departments for their verification. Additionally, we reviewed the language in the strategy and HSPDs to determine which departments had been identified as lead agencies in implementing the initiatives. In some cases, the leadership language was clear; in other cases, it was less precise or implied. We were then able to determine whether departments demonstrated planning or implementation activities in both lead and nonlead initiatives. Our analysis is necessarily a snapshot of activity as of particular points in time. The agencies reviewed provided us with information as to their planning and implementation as of various dates, including fiscal year 2004. We recognize that the agencies continue to plan and implement their strategies and programs and have and may continue to progress beyond the status portrayed in this analysis. Finally, our work did not assess the status or quality of the work being planned or implemented.

To determine homeland security challenges facing the nation, we reviewed our reports issued since September 11. This included over 250 products cutting across the gamut of homeland security activities. We summarized and categorized the challenges by critical mission area and subtopic where appropriate (e.g., the Border and Transportation Security mission area was subdivided into border security and transportation security). While our summary is limited to challenges we identified, we have noted in the text where the congressionally chartered commissions have raised similar issues. We recognize that these commissions, Congress, the executive branch, and other organizations have identified additional challenges in each of the mission areas.

We conducted our work between February and November 2004 in accordance with generally accepted government auditing standards. For more details on our objectives, scope, and methodology, see appendix I.

## Agency Plans, Implementation, and Challenges

The following sections provide summaries of each mission area, as well as issues that cut across all six mission areas. These summaries include an analysis of federal departments' strategic planning and implementation activities and the challenges faced by these departments and the nation as a whole.

### Intelligence and Warning

The strategy identifies five initiatives under the Intelligence and Warning mission area. All of the initiatives are covered by at least two departments planning or implementation activities (see table 1). Examples include DOJ and DOE activities to enhance the analytic capabilities of the Federal

Bureau of Investigation (FBI); DHS, State, and DOE activities to utilize dual-use analysis to prevent attacks; and DHS, DOD, and DOE activities to employ red-team techniques.

Four of the five initiatives have a department identified as a lead agency. Neither the strategy nor the HSPDs identified a lead agency on the fifth initiative, which relates to the employment of red-team techniques. According to DHS strategic planning officials, it is important that a number of agencies conduct red-team techniques to test their own specific programs, so no agency would necessarily have the overall lead. See appendix II for a more detailed discussion on the implications of not having an overall lead agency identified for red-team techniques. For this mission area, the lead agency specifications are clear (rather than implied), and there are no multiple leads on any of the initiatives.

All five initiatives were being implemented in fiscal year 2004 as reported by two or more departments (see table 7). DHS and DOJ cited 2004 implementation activity for each of the initiatives for which they were identified as lead agencies.

**Table 1: Department Leadership, Planning, or Implementation Activity in the Intelligence and Warning Mission Area's Five Initiatives**

| | DHS | DOJ | DOD | HHS | State | DOE |
|---|---|---|---|---|---|---|
| **Intelligence and warning** | | | | | | |
| (1) Enhance analytic capabilities of the FBI | | ● | | | | ● |
| (2) Build new capabilities through the Information Analysis and Infrastructure Protection Division of the proposed DHS | ● | | ● | | | ● |
| (3) Implement the Homeland Security Advisory System | ● | | ● | | | ● |
| (4) Utilize dual-use analysis to prevent attacks | ● | | | | ● | ● |
| (5) Employ red-team techniques | ● | | ● | | | ● |

● Indicates the department has planning and/or implementation activity related to this initiative

▭ Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Source: GAO.

Refer to appendix II for more specific details regarding department planning and implementation activities, including a discussion of fiscal year 2004 implementation. As explained further in appendix II, we did not include CIA in our analysis because of the lack of funding data and because the strategy provides little discussion of the agency.

Our work in the Intelligence and Warning mission area since 2001 has highlighted a number of challenges that need to be addressed. Many of these challenges are directly related to initiatives in this mission area. These challenges include

- improving analysis capabilities at the FBI through better strategic information management,
- developing productive information-sharing relationships among the federal government and state and local governments and the private sector,
- overcoming the limitations in the sharing of classified national security information across sectors,
- ensuring that the private sector receives better information on potential threats,

- consolidating watch lists to promote better information and sharing, and

- maintaining a viable and relevant homeland security advisory system.

These challenges are discussed in greater detail in appendix II. Many of these challenges were also discussed by one or more of the Bremer, Gilmore, Hart-Rudman, and 9/11 Commissions.

## Border and Transportation Security

There are six initiatives under the Border and Transportation Security mission area. All of the initiatives are covered by at least two departments' planning or implementation activities (see table 2). Examples include DHS, DOD, HHS, State, and DOE activities to ensure accountability in border and transportation security; DHS, DOD, State, and DOE activities to increase the security of international shipping containers; and DHS, DOJ, and State activities to reform immigration services.

All six initiatives have a department identified as a lead agency. One initiative (i.e., creating smart borders) has multiple lead agencies identified in the strategy and HSPDs. DHS is a lead on the most initiatives: a clear lead on two initiatives and an implied lead on four other initiatives.

All six initiatives were being implemented in fiscal year 2004 as reported by one or more departments (see table 8). DHS and State cited 2004 implementation activity in each of the initiatives for which they were identified as leads. DOJ had been identified as a lead agency with respect to creating smart borders and reforming immigration services, but with the transfer of the Immigration and Naturalization Service to DHS, DOJ officials indicated that the department was no longer serving as a lead on that initiative.

**Table 2: Department Leadership, Planning, or Implementation Activity in the Border and Transportation Security Mission Area's Six Initiatives**

| | DHS | DOJ | DOD | HHS | State | DOE |
|---|---|---|---|---|---|---|
| **Border and transportation security** | | | | | | |
| (1) Ensure accountability in border and transportation security | ● | | ● | ● | ● | ● |
| (2) Create "smart borders" | ● | ● | | ● | ● | |
| (3) Increase the security of international shipping containers | ● | | ● | | ● | ● |
| (4) Implement the Aviation and Transportation Security Act of 2001 | ● | | ● | | | |
| (5) Recapitalize the U.S. Coast Guard | ● | | ● | | | |
| (6) Reform immigration services | ● | ● | | | ● | |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Department IMPLICITLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Source: GAO.

Refer to appendix III for more specific details regarding department planning and implementation activities, including a discussion of fiscal year 2004 implementation.

Border and Transportation Security is another mission area where our work has indicated there are challenges to be addressed. Again, many of these challenges are directly related to initiatives in this mission area. These challenges include

- striking an acceptable balance between security and the flow of commercial activity, travel, and tourism;
- processing people at our nation's land ports of entry and determining the proper role of biometric technologies for security applications;
- deploying the best available technologies for detecting radioactive and nuclear materials at U.S. ports of entry;
- developing a clear and comprehensive policy on the use of visas as an antiterrorism tool and improving the management and oversight of programs to track visitors;

- implementing an effective system to prescreen passengers prior to their arrival at the airport, as well as achieving and sustaining improvements in airline passenger and baggage screening; and

- strengthening perimeter security at airports and countering the threat of hand-held missiles to commercial aviation.

These and other challenges are discussed in greater detail in appendix III. Many of these challenges were also discussed by one or more of the Bremer, Gilmore, Hart-Rudman, and 9/11 Commissions.

## Domestic Counterterrorism

The Domestic Counterterrorism mission area has six initiatives. All of the initiatives are covered by at least one department's planning or implementation activities (see table 3). Examples include DHS, DOJ, DOD, HHS, and DOE activities to improve intergovernmental law enforcement coordination; DHS, DOJ, DOD, and State activities to facilitate apprehension of potential terrorists; and DHS, DOJ, and State activities to target and attack terrorist financing.

Each of the six initiatives has a department that is identified as a lead agency. All indicated leads from the strategy and HSPDs are clear leads. For three of the six initiatives, multiple departments have been identified as leads.

All 6 initiatives were being implemented in fiscal year 2004 as reported by one or more departments (see table 9). DOJ cited 2004 implementation activity on each of the six initiatives for which it was identified as a lead. DHS and State also cited implementation activity on all initiatives for which they were identified as lead agencies.

**Table 3: Department Leadership, Planning, or Implementation Activity in the Domestic Counterterrorism Mission Area's Six Initiatives**

| | DHS | DOJ | DOD | HHS | State | DOE |
|---|---|---|---|---|---|---|
| **Domestic counterterrorism** | | | | | | |
| (1) Improve intergovernmental law enforcement coordination | ● | ● | ● | ● | | ● |
| (2) Facilitate apprehension of potential terrorists | ● | ● | ● | | ● | |
| (3) Continue ongoing investigations and prosecutions | ● | ● | | | | |
| (4) Complete FBI restructuring to emphasize prevention of terrorist attacks | | ● | | | | |
| (5) Target and attack terrorist financing | ● | ● | | | ● | |
| (6) Track foreign terrorists and bring them to justice | ● | ● | ● | | ● | ● |

● Indicates the department has planning and/or implementation activity related to this initiative

▭ Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Source: GAO.

Refer to appendix IV for more specific details regarding department planning and implementation activities, including a discussion of fiscal year 2004 implementation.

Domestic Counterterrorism is another mission area where our recent work has highlighted continuing challenges. These challenges threaten to undermine law enforcement agencies' ability to aggressively detect, deter, prevent, eradicate, and adjudicate terrorist activity. These challenges include

- transforming the FBI from an investigative organization into a proactive entity focused on detecting and preventing terrorist activity,
- modifying the FBI's related workforce and business practices to focus on counterterrorism and intelligence-related priorities,
- improving interagency coordination to leverage existing law enforcement resources to investigate money laundering and terrorist financing,
- monitoring the use of alternate financing mechanisms by terrorists,
- identifying and apprehending terrorists already present in the United States, and
- recognizing counterfeit documentation and the use of identity fraud at U.S. borders and other security checkpoints.

These challenges are discussed in greater detail in appendix IV. Many of these challenges were also discussed by one or more of the Bremer, Gilmore, Hart-Rudman, and 9/11 Commissions.

## Protecting Critical Infrastructures and Key Assets

The strategy identifies eight initiatives under the Protecting Critical Infrastructures and Key Assets—commonly referred to as Critical Infrastructure Protection (CIP)— mission area. All of the initiatives are covered by at least four departments' planning or implementation activities (see table 4). Examples include DHS, DOJ, DOD, HHS, and DOE activities to unify America's infrastructure protection effort in DHS; DHS, DOD, HHS, and DOE activities to develop a national infrastructure protection plan and, all six departments' activities to secure cyberspace.

Each of the eight initiatives has a department identified as a lead agency. In the case of five of the eight initiatives, the leads are clear; only in the case of three initiatives (i.e., enabling effective partnership with state and local governments and the private sector, securing cyberspace, and partnering with the international community to protect our transnational infrastructure) are there implied leads. For three of the eight initiatives, multiple lead agencies have been identified. For example, DOD, HHS, and DOE are all sector leads on the same initiative—building and maintaining a complete and accurate assessment of America's critical infrastructure and key assets. These departments have the sector leads as follows, DOD for defense industrial base, HHS for public health, and DOE for the energy sector.

All eight initiatives were being implemented in fiscal year 2004 as reported by two or more departments (see table 10). DHS, DOD, HHS, State, and DOE cited implementation activity on all initiatives for which they were identified as lead agencies.

**Table 4: Department Leadership, Planning, or Implementation Activity in the Critical Infrastructure Protection Mission Area's Eight Initiatives**

| | DHS | DOJ | DOD | HHS | State | DOE |
|---|---|---|---|---|---|---|
| **Protecting critical infrastructures and key assets** | | | | | | |
| (1) Unify America's infrastructure protection effort in DHS | ● | ● | ● | ● | | ● |
| (2) Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets | ● | ● | ● | ● | | ● |
| (3) Enable effective partnership with state and local governments and the private sector | ● | ● | ● | ● | | ● |
| (4) Develop a national infrastructure protection plan | ● | | ● | ● | | ● |
| (5) Secure cyberspace | ● | ● | ● | ● | ● | ● |
| (6) Harness the best analytic and modeling tools to develop effective protective solutions | ● | | ● | ● | | ● |
| (7) Guard America's critical infrastructure and key assets against "inside" threats | ● | | ● | ● | ● | ● |
| (8) Partner with the international community to protect our transnational infrastructure | ● | ● | ● | ● | ● | |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Department IMPLICITLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Source: GAO.

Refer to appendix V for more specific details regarding department planning and implementation activities, including a discussion of fiscal year 2004 implementation.

Our work related to CIP has identified several challenges. Overcoming the challenges presented in this mission area is made even more difficult because increasing the security of one type of target, such as aircraft or federal buildings, increases the possibility that terrorists may choose another type of target, such as trains or ports. The challenges include

- refining the federal government's role in managing CIP;
- developing a comprehensive and coordinated national CIP plan that delineates the roles, defines interims objectives and milestones, sets time frames, and establishes performance measures;

- developing productive information-sharing relationships within the federal government and among federal, state, and local governments and the private sector;

- improving the federal government's capabilities to analyze incident, threat, and vulnerability information related to critical infrastructures and key assets;

- improving the security of government facilities through a variety of methods, including better training and procedures to detect counterfeit documents and identity fraud; and

- analyzing the strengths, interdependencies, and vulnerabilities of several specific industries, including the financial services sector, the shipping and postal system, drinking water, agriculture, the chemical industry, nuclear power plants, and nuclear weapons sites.

These challenges are discussed in greater detail in appendix V. Many of these challenges were also discussed by one or more of the Bremer, Gilmore, Hart-Rudman, and 9/11 Commissions.

## Defending Against Catastrophic Threats

There are six initiatives under the Defending against Catastrophic Threats mission area. All of the initiatives are covered by at least two departments' planning or implementation activities (see table 5). Examples include DHS, DOD, State, and DOE activities to prevent terrorist use of nuclear weapons through better sensors and procedures; DHS, DOD, HHS, and DOE activities to detect chemical and biological materials and attacks; and DHS, DOD, HHS, State, and DOE activities to harness the scientific knowledge and tools to counter terrorism.

Each of the six initiatives has a department identified as a lead agency. On half the initiatives, multiple departments have been identified as leads. In the case of three initiatives, the leads are clear; in the case of the remaining three initiatives, several leads are implied.

All six initiatives were being implemented in fiscal year 2004 as reported by one or more departments (see Table 11). DHS cited implementation activity in five of the six initiatives for which it was identified as a lead. It is not yet implementing the Select Agent Program. DOD, HHS, State, and DOE cited implementation activity on all the initiatives for which they were identified as the lead agency.

**Table 5. Department Leadership, Planning, or Implementation Activity in the Defending Against Catastrophic Threats Mission Area's Six Initiatives**

| | DHS | DOJ | DOD | HHS | State | DOE |
|---|---|---|---|---|---|---|
| **Defending against catastrophic threats** | | | | | | |
| (1) Prevent terrorist use of nuclear weapons through better sensors and procedures | ● | | ● | | ● | ● |
| (2) Detect chemical and biological materials and attacks | ● | | ● | ● | | ● |
| (3) Improve chemical sensors and decontamination techniques | ● | | | ● | | ● |
| (4) Develop broad spectrum vaccines, antimicrobials, and antidotes | ● | | | ● | ● | ● |
| (5) Harness the scientific knowledge and tools to counter terrorism | ● | | ● | ● | ● | ● |
| (6) Implement the Select Agent program | | | ● | ● | | |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Department IMPLICITLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Source: GAO.

Refer to appendix VI for more specific details regarding department planning and implementation activities, including a discussion of fiscal year 2004 implementation.

The challenges the nation faces in defending itself against catastrophic threats—such as the terrorist use of chemical, biological, radiological, or nuclear (CBRN) weapons—are quite broad and could have devastating consequences if not effectively addressed. Our recent work in this mission area has highlighted challenges that include

- strengthening efforts to keep weapons of mass destruction (WMD) and dual-use items (items having both commercial and military applications) out of the hands of terrorists,
- controlling the sale of excess items that can be used to produce and deliver biological agents, and
- designating lead agencies for setting priorities for information systems related to terrorism.

These challenges are discussed in greater detail in appendix VI. Many of these challenges were also discussed by one or more of the Bremer, Gilmore, Hart-Rudman, and 9/11 Commissions.

## Emergency Preparedness and Response

For the Emergency Preparedness and Response mission area, the strategy identifies 12 initiatives. All of the initiatives are covered by at least two departments' planning or implementation activities (see table 6). Examples include DHS, DOD, HHS, and DOE activities to create a national incident management system; DHS and HHS activities to enable seamless communications among all responders; and, DHS, DOD, HHS, and DOE activities to augment America's pharmaceutical and vaccine stockpiles.

Each of the 12 initiatives has a department identified as a lead agency. For 3 of the 12 initiatives, multiple lead agencies have been identified. All leads, with three exceptions, are clear leads.

All 12 initiatives were being implemented in fiscal year 2004 by two or more departments (see table 12). DHS, DOD and HHS cited implementation activity in 2004 for all initiatives for which they were identified as lead agencies.

**Table 6: Department Leadership, Planning, or Implementation Activity in the Emergency Preparedness and Response Mission Area's Twelve Initiatives**

| | DHS | DOJ | DOD | HHS | State | DOE |
|---|---|---|---|---|---|---|
| **Emergency preparedness and response** | | | | | | |
| (1) Integrate separate federal response plans into a single all-discipline incident management plan | ● | | ● | ● | | ● |
| (2) Create a national incident management system | ● | | ● | ● | | ● |
| (3) Improve tactical counter terrorist capabilities | ● | | ● | ● | ● | ● |
| (4) Enable seamless communication among all responders | ● | | | ● | | |
| (5) Prepare health care providers for catastrophic terrorism | ● | | ● | ● | | ● |
| (6) Augment America's pharmaceutical and vaccine stockpiles | ● | | ● | ● | | ● |
| (7) Prepare for chemical, biological, radiological, and nuclear decontamination | ● | | ● | ● | | ● |
| (8) Plan for military support to civil authorities | ● | | ● | | | |
| (9) Build the Citizen Corps | ● | ● | | | | |
| (10) Implement the first responder initiative of the fiscal year 2003 budget | ● | ● | | | | |
| (11) Build a national training and evaluation system | ● | ● | ● | ● | | |
| (12) Enhance the victim support system | ● | ● | | ● | | |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Department IMPLICITLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Source: GAO.

Refer to appendix VII for more specific details regarding department planning and implementation activities, including a discussion of fiscal year 2004 implementation.

Our recent work has shown that there are many challenges in the Emergency Preparedness and Response mission area regarding efforts to effectively minimize the damage and successfully recover from terrorist attacks. We identified the following challenges:

- adopting an "all hazards" approach to emergency preparedness and response;
- providing better governmental planning and coordination with regard to first responder issues;
- preparing first responders for incidents involving catastrophic terrorism;
- restructuring the federal grant system for first responders;
- strengthening public health in a variety of areas, including better information sharing, preparations for catastrophic terrorism such as bioterrorism, and more hospital equipment;
- improving regional response planning involving multiple municipalities, states, and countries;
- establishing and implementing preparedness standards and measures;
- ensuring adequate communications among first responders and with the public; and
- defining the roles and responsibilities of DOD in defending the homeland and providing military support to civil authorities.

These challenges are discussed in greater detail in appendix VII. Many of these challenges were also discussed by one or more of the Bremer, Gilmore, Hart-Rudman, and 9/11 Commissions.

## Crosscutting Issues

Our recent work has also identified homeland security challenges that cut across the various mission areas. While it is important that the major mission challenges be individually addressed, it is equally important that these challenges be addressed from a comprehensive national homeland security perspective (i.e., some mission areas overlap, some challenges are common across mission areas, some corrective actions have ramifications, and there are both positive and negative challenges across mission area boundaries). Coordinated actions may substantially enhance multiple mission performance. The *National Strategy for Homeland Security* and the corresponding strategic plans of the agencies accountable for achieving the national strategy's objectives must address and resolve the sometimes competing issues among homeland security mission areas and between homeland security and other important national priorities and objectives. These crosscutting issues are often the most difficult to address. Some of these challenges that we have identified are governmentwide in nature—they cut across the federal, state, and local governments, and sometimes private sectors. Such governmentwide challenges that we have identified include

- balancing homeland security needs with other national requirements by formulating realistic budget and resource plans that support the implementation of an efficient and effective homeland security program;

- providing timely and transparent homeland security funding information that sets forth detailed information concerning the obligation of the funding provided;

- improving risk management methods for resource allocation and investments by developing a commonly accepted framework and supporting tools to guide agency analysts in providing information to management;

- establishing baseline performance goals and measures upon which to assess and improve prevention efforts, evaluate vulnerability reduction, and gauge responsiveness to damage and recovery needs at all levels of government;

- clarifying the roles and responsibilities within and between the levels of government and the private sector through the development and implementation of an overarching framework and criteria to guide the process;

- developing a national blueprint—called an enterprise architecture—to help integrate different organizations' efforts to improve homeland security; and

- improving governmentwide information technology management through the consistent application of effective strategic planning and performance measurement practices.

These challenges are discussed in greater detail in appendix VIII. Many of these challenges were also discussed by one or more of the Bremer, Gilmore, Hart-Rudman, and 9/11 Commissions.

In addition to the challenges discussed earlier, DHS—as the department most responsible for Homeland Security—faces a number of challenges. Because of this, in January 2003, we designated the overall implementation and transformation of DHS as high-risk.[9] We gave it this designation for

[9]See GAO, *Major Management Challenges and Program Risks, Department of Homeland Security*, GAO-03-102 (Washington, D.C.: Jan. 24, 2003).

three reasons. First, the size and complexity of the effort make the challenge especially daunting, requiring sustained attention and time to achieve the department's mission in an effective and efficient manner. Second, the components being merged into DHS already face a wide array of existing challenges that must be addressed. Finally, if DHS cannot effectively carry out its mission, it exposes the nation to potentially very serious consequences. We are currently in the process of reviewing the challenges faced by DHS and the progress it has made to address these challenges. The results of this review will be published in a forthcoming GAO report.

## Concluding Observations

All 43 initiatives of the *National Strategy for Homeland Security* were included in plans and implementation activities in fiscal year 2004 by at least one of the six key departments we reviewed. Further, 33 of the 43 initiatives (77 percent) were being planned or implemented by at least three of the six departments. Additionally, we found that the strategy and HSPDs identified lead agencies for 42 of the 43 initiatives. For these 42 initiatives where a lead had been identified, 13 initiatives had leads that were implied rather than clear. While DHS was identified as the lead for the most initiatives (37), there were multiple leads for 12 of these 42 initiatives. Given the large number of initiatives being implemented by multiple agencies, the fact that some of the leads were implied rather than clear, and the fact that about a third of the initiatives had multiple leads, coordination across federal departments will be a key factor required for the successful implementation of the strategy. Such coordination would ensure that federal departments are working to support the lead agency, are complementing one anothers' leadership when there are multiple lead agencies, and are not unnecessarily duplicating one anothers' programs when there are multiple departments implementing the same initiatives.

When implementing the strategy's initiatives, these federal departments face a number of challenges that cut across all the mission areas. In terms of resources, the nation must find the appropriate balance between homeland security and other priorities. Finding this balance will require an improved risk management framework for resource allocation and investments. It will also require an improved set of performance and results measures to gauge our progress. Further, finding that balance must take into consideration nonfederal resources, but the strategy and HSPDs have not in many cases defined the roles and responsibilities of the state, local, and private sectors. Finally, an enterprise architecture would help coordinate the larger effort across the myriad of organizations involved in implementing the strategy.

One of the key challenges for the Congress is to provide oversight to ensure that federal departments are coordinating their activities as they attempt to implement the *National Strategy for Homeland Security*.

## Agency Comments and Our Evaluation

We provided a draft of this report to DOD, DOE, DOJ, HHS, DHS, the State Department, and the Homeland Security Council for comment. We received written comments from DOD, HHS, DHS, and DOJ, which appear in appendixes XI –XIV respectively. In addition to providing their written comments, these departments and DOE provided technical comments, which we incorporated as appropriate. State and the Homeland Security Council declined to provide any comments on this report. DOD stated that the report was "a thorough and accurate report." DHS indicated our summation of the strategic planning, implementation, and leads of the six departments to be "particularly useful." DOE, DOJ, and HHS neither concurred nor disagreed with the report. In addition, agencies provided comments on the many GAO reports that cumulatively describe the range of implementation challenges featured in this capping report. These comments can be found in the appropriate reports, as cited in our footnotes and listed in the Related GAO Products section.

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after its issue date. At that time, we will provide copies of this report to appropriate departments and interested congressional committees. 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 have any questions about this report, please contact me on 512-6787. Other contacts and staff acknowledgments are listed in appendix XV.

Sincerely yours,

Norman J. Rabkin
Managing Director
Homeland Security and Justice Issues

# Appendix I: Objectives, Scope, and Methodology

The first objective focuses on the extent to which key federal departments with homeland security responsibilities address the 43 initiatives of the *National Strategy for Homeland Security* in their planning and implementation activities.

We selected departments based on a review of their fiscal year 2005 budget requests for homeland security-related issues. The six departments with the largest budget requests were selected—together they account for 94 percent of the fiscal year 2005 budget requests for homeland security. The six departments are the Departments of Defense (DOD), Energy (DOE), Health and Human Services (HHS), Homeland Security (DHS), Justice (DOJ), and State.

We defined three time-oriented indicators to distinguish the timing of the departments' strategic planning or implementation activities with respect to each of the 43 initiatives of the six mission areas.

- "Prior implementation" was defined as a departmental program or activity that occurred prior to fiscal year 2004.

- "Recent planning" was defined as either (1) a program or activity specifically indicated by the participating department as being developed in its latest high-level planning documents (which include the department's strategic plan, annual plan, or performance plan) or (2) a program or activity, not listed in these planning documents, but indicated by department officials as being under development since July 2002 (when the strategy was issued).

- "2004 implementation," in turn, was defined as a departmental program or activity that occurred during all, or part, of fiscal year 2004.

A department could satisfy (a) neither of these indicators (demonstrating no strategic planning and implementation activities on a given initiative, within the prescribed time periods) or (b) combinations of one through three of these indicators, for each initiative (e.g., one department may have engaged in prior implementation that was carried over into fiscal year 2004 implementation; a second department may have engaged in recent planning, followed by 2004 implementation; and a third department may have only engaged in prior implementation, as its activity was completed or terminated.)

We obtained and reviewed each department's latest strategic planning documents (i.e., their strategic plan, annual plan, and performance plan) to determine whether these documents provided specific information about the department's prior implementation and recent planning activities, with respect to each mission area initiative. We scored a department as engaging in prior implementation activity or recent planning if these documents demonstrated at least one such activity with respect to each initiative. We also reviewed the documents to determine if any programs or activities had been transferred to another department or agency. In some cases, this may account for prior implementation activity but no further planning or implementation activity.

Since the latest departmental strategic documents do not sufficiently address fiscal year 2004 implementation activities, we contacted strategic planning officials at each the six departments and asked them to provide evidentiary support for their 2004 implementation activities, with respect to each relevant initiative. We scored a department as implementing activities on a given initiative if the department could demonstrate at least one such activity occurring during fiscal year 2004 with respect to that initiative. We also requested department strategic planning officials to review our findings regarding planning and implementation and to make any modifications or additions necessary. Evidentiary support was requested for any such change. Very few changes were provided across all six departments. Departments provided the data during fiscal year 2004. We did not verify the accuracy of the data or the progress of particular activities.

In addition to identifying departmental engagement in planning and implementation activities, we also sought to determine departmental leadership responsibility on each initiative. To satisfy the leadership role, departments had to satisfy at least one of the following two indicators:

- leadership of the entire critical mission area initiative or
- leadership in specific functional area(s) encompassed within that initiative.

We identified departmental leadership roles on specific initiatives, based on a review of the provisions in the strategy and Homeland Security Presidential Directives (HSPD) one through 12. In only a few instances did a department indicate to us that subsequent legislation, regulation, or transfer of activities absolved them of their leadership roles. Because the language of the strategies and HSPDs was not always precise, we

identified departments as either (a) “clear” (explicit) leads, (b) “implied” leads, or (c) no leads for each initiative. In the mission area tables, in both the letter and appendixes, departments with a clear lead on a given initiative are indicated by a hard-line box; departments with an implied lead on a given initiative are indicated by a broken-line box; departments not having any lead on a given initiative have no box designations. Drafts of this section of the report were submitted to the departments for their review.

The second objective focuses on identifying the challenges the nation faces in homeland security implementation. This work is based exclusively on a review of challenges identified in GAO products issued since September 11, 2001. During this time period, we were able to identify over 250 relevant GAO products related to homeland security. These, and others, can be found in our Related Products section at the end of the report. The challenges identified are arrayed throughout the report by mission area and subtopical area.

We conducted our work between February and November 2004 in accordance with generally accepted government auditing standards.

# Appendix II: Intelligence and Warning

This appendix sets forth the definition and major initiatives of the Intelligence and Warning mission area and discusses the agencies with major roles, their funding, and the alignment of their strategic plans and implementation activities with the initiatives, and a summary of the key challenges faced by the nation. This appendix presents baseline information that can be used by Congress to provide oversight and track accountability for the initiatives in the Intelligence and Warning mission area.

## Definition and Major Initiatives

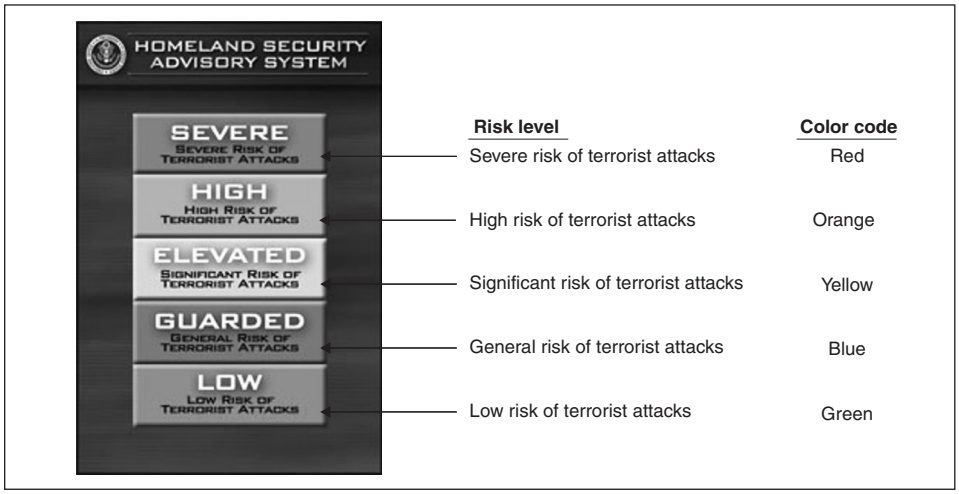
The *National Strategy for Homeland Security* categorizes homeland security activities into six critical mission areas, the first of which is Intelligence and Warning. This mission area includes intelligence programs and warning systems that can detect terrorist activity before it manifests itself in an attack so that proper preemptive, preventive, and protective action can be taken. Specifically, this mission area is made up of efforts to identify, collect, analyze, and distribute source intelligence information or the resultant warnings from intelligence analysis. Activities in this mission area often dovetail into the mission areas of domestic counterterrorism and, in some cases, critical infrastructure protection, as agencies move to take immediate action or develop long-term protective measures based on threat or vulnerability information.[1] Figure 3 is an example of one of the initiatives found in the Intelligence and Warning mission area.

The strategy identifies the following initiatives in the Intelligence and Warning mission area:

- enhancing the analytic capabilities of the FBI,
- building new capabilities through the Information Analysis and Infrastructure protection Division of the Department of Homeland Security,
- implementing the Homeland Security Advisory System,
- utilizing dual-use analysis to prevent attacks, and
- employing red team techniques.

[1]This definition is from the Office of Management and Budget's (OMB) *2003 Report to Congress on Combating Terrorism* (Washington, D.C.: Sept. 2003).

**Figure 3: The Five Threat Levels of the Homeland Security Advisory System**




Source: DHS.

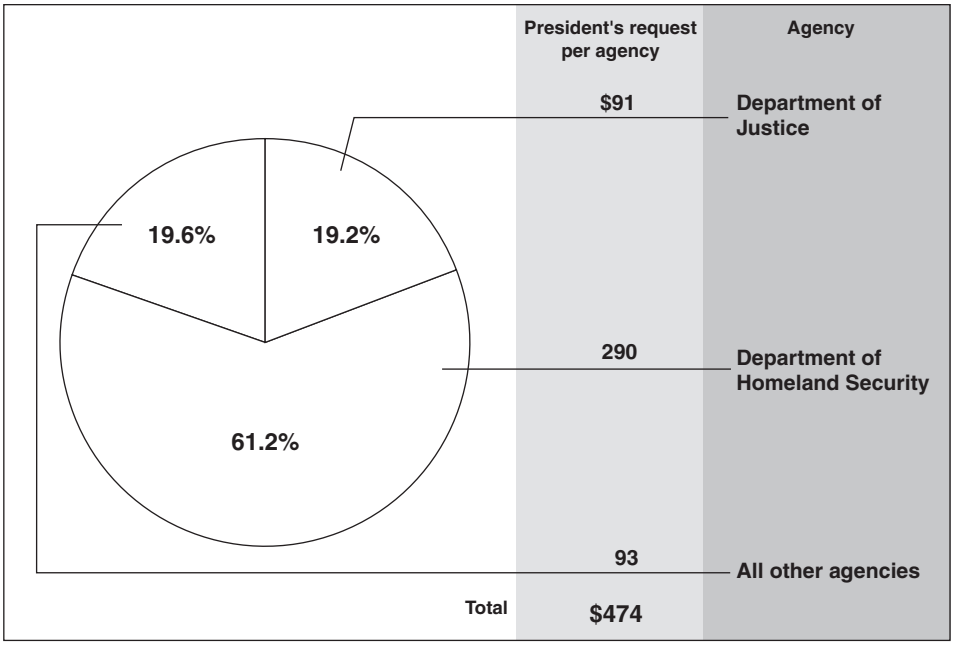
## Agencies with Major Roles in Intelligence and Warning

Of the six departments under review, the Department of Homeland Security and the Department of Justice have major roles in the Intelligence and Warning mission area. Within DHS, the Information Analysis and Infrastructure Protection Directorate (IAIP) analyzes terrorism-related threat information relevant to homeland security, associates threat analysis with infrastructures and people, and provides warnings and advisories to agencies, state and local governments, and select critical infrastructure owners and operators. The U.S. Secret Service, also a component of DHS, provides intelligence and advanced analysis for protective operations. The Department of Justice has two components involved in Intelligence and Warning activities—the Federal Bureau of Investigation (FBI) shares intelligence with other federal agencies, as well as with state and local authorities; while the Office of Justice Programs (OJP) funds counterterrorism training for senior law enforcement personnel at the state and local level.

The Office of Management and Budget (OMB) reported that the total fiscal year 2005 funding request for the Intelligence and Warning mission area is $474 million, with the bulk of this funding going to DHS (61 percent), primarily for IAIP and the U.S. Secret Service. Other agencies with significant funding in this mission area include DOJ (19 percent), primarily for the FBI, and the Intelligence Community (15 percent) for the Terrorist

Threat Integration Center (TTIC).[2] Figure 4 summarizes the fiscal year 2005 budget request for the Intelligence and Warning mission area by agency.

**Figure 4: Proposed Fiscal Year 2005 Homeland Security Funding for Intelligence and Warning**




Source: GAO, based on OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005.*

Notes: Budget authority in millions of dollars.

"All other agencies" includes the Departments of Agriculture ($20 million) and Treasury ($.6 million), as well as the Intelligence Community Management Account ($72 million). OMB reported the Intelligence Community figure in aggregate; it did not break it out by individual agencies (e.g., Central Intelligence Agency).

OMB's reported data does not include funding for three departments that have activities under way in this mission area. These departments—Defense, State, and Energy—have either planning or implementation activity on specific initiatives, as discussed in the next section of this appendix. On the basis of our previous work, we have noted several

[2]OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005* (Washington, D.C.: Feb. 2004). OMB did not break the Intelligence Community spending down to the level of individual agencies.

qualifications to OMB's figures to explain this discrepancy.[3] According to OMB officials, there is not always a clear distinction between homeland security activities and other related activities. The OMB staff must make judgment calls about how to characterize funding by mission areas. For example, some homeland security activities have multiple purposes, so funding for these activities can be allocated among several accounts covering multiple mission areas. Moreover, some of the departments' activities, such as planning, coordination, or providing advice may support Intelligence and Warning activities, but are not included in the amounts shown.

This appendix does not have any discussion of the Central Intelligence Agency (CIA) or the Intelligence Community as a whole, although they have activities related to the Intelligence and Warning mission area. There are two reasons for this omission. First, OMB's reported data do not include funding for the CIA. Second, the strategy itself is relatively silent on the CIA in terms of specific initiatives in this mission area. For example, the strategy only mentions the CIA once in the Intelligence and Warning mission area—the CIA was to provide intelligence analysts to assist the FBI enhance its analytic capabilities. Most of the initiatives in the strategy, as discussed in the next section, are led by DHS or DOJ. Similarly, there is little information on the Intelligence Community. While OMB reported data include $72 million in spending by the Intelligence Community Management Account, it does not break this amount out by specific departments or agencies. While the strategy mentions the Intelligence Community with respect to this mission area, it does not identify specific departments or agencies with specific initiatives. One potential reason for relatively little discussion of CIA and the Intelligence Community is the unclassified nature of the cost data and the strategy.

## Alignment of Department Activities with the Major Initiatives

This section provides more detailed information about the Intelligence and Warning mission area initiatives, and the departments involved in conducting activities related to these initiatives. This includes a discussion of specific departmental planning and implementation activities, lead agency designation, and implementation activities in fiscal year 2004, with respect to each initiative. The data are summarized in table 7.

[3]See GAO, *Combating Terrorism: Funding Data Reported to Congress Should Be Improved*, GAO-03-170 (Washington, D.C.: Nov. 26, 2002).

**Table 7: Detailed Department Leadership and Planning/Implementation Activities in the Intelligence and Warning Mission Area's Five Initiatives**

| | DHS | | | DOJ | | | DOD | | | HHS | | | State | | | DOE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 |
| **Intelligence and warning** | | | | | | | | | | | | | | | | | | |
| (1) Enhance analytic capabilities of the FBI | | | | ● | ● | ● | | | | | | | | | | ● | | ● |
| (2) Build new capabilities through the Information Analysis and Infrastructure Protection Division of the proposed DHS | | ● | ● | | | | | | ● | | | | | | | ● | | ● |
| (3) Implement the Homeland Security Advisory System | | ● | ● | | | | | | ● | | | | | | | ● | | ● |
| (4) Utilize dual-use analysis to prevent attacks | | ● | ● | | | | | | | | | | ● | ● | ● | | ● | |
| (5) Employ "red-team" techniques | | ● | ● | | | | ● | | ● | | | | | | | | | ● |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

PI = Prior implementation to fiscal year 2004
RP = Recent planning
04 = Fiscal year 2004 implementation

Source: GAO.

## Summary of Departmental Activities on the Initiatives

All five Intelligence and Warning initiatives are being addressed in at least two of the key departments' planning and implementation activities (see table 7). For example, DHS, DOD, and DOE implemented Homeland Security Advisory System initiative activities during fiscal year 2004. More specifically, DHS implemented the system and issued advisories; DOD personnel interacted with DHS; and DOE aligned its security system and condition alert level to meet the Homeland Security Advisory System requirements of DHS. In addition, DHS, DOD, and DOE implemented new intelligence and warning capabilities through the IAIP initiative of DHS during fiscal year 2004. Specifically, DHS conducted assessments of critical infrastructures and key assets using the IAIP system; DOD worked in conjunction with DHS on the IAIP system; and DOE enacted a Safeguard and Security Program (using infrastructure information and analysis to gauge vulnerability assessments) and plays a role in disseminating threat information to energy sector industries.

The Department of Health and Human Services (HHS) also has activities related to Intelligence and Warning, but these activities are not directly included under the initiatives as laid out by the strategy. For example HHS operates the Laboratory Response Network, the Epidemic Information

Exchange, and the Food and Drug Administration's food inspection activities. In addition, it supports the DHS-managed BioWatch program. While the strategy does not list these as specific initiatives, they provide surveillance of infectious diseases and could provide early warning of a bioterrorism attack. For more on HHS's role, particularly with respect to bioterrorism, see appendix VI, on Defending against Catastrophic Threats.

While we have identified department activities related to these initiatives, we did not determine the quality, status, or progress of such activities with respect to stated goals or targets within this mission area.

## Identification of Lead Agencies on the Initiatives

For four of the five initiatives, a lead agency is identified either in the strategy or Homeland Security Presidential Directives (HSPDs). The one initiative where there was no lead identified was "the employment of red-team techniques." Red team techniques are techniques where the U.S. government would create a team (sometimes known as a red cell) to play the role of terrorists in terms of identifying vulnerabilities and planning attacks. Three departments (DHS, DOD, and DOE) had implemented activities related to this initiative. According to DHS strategic planning officials, it is important that a number of agencies conduct red-team techniques to test their own specific programs, so no agency would necessarily have the overall lead. However, terrorists are opportunistic and may purposefully plan attacks that take advantage of the seams between department programs or jurisdictions. Thus, there is some value in employing red-team techniques that look across federal departments, as well as across the state, local, and private sectors. Without an overall lead agency identified for this initiative, it is unclear which federal department will be accountable for employing red-team techniques at the interagency level against the nation as a whole.

As shown in table 7, DHS is the lead on the most initiatives in this critical mission area—three out of the five initiatives (including building new capabilities through the Information Analysis and Infrastructure Protection Division, implementing the Homeland Security Advisory System, and utilizing dual-use analysis to prevent attacks). It is understandable that DHS would be the department with the most initiative leads given that DHS's strategic goals and objectives are to be directed toward preventing terrorist attacks in the United States and reducing America's vulnerability to terrorism—both of which require Intelligence and Warning system information to achieve their aims. The Department of Justice is a lead on one initiative, enhancing the analytic capabilities of the

FBI. This, too, is understandable given that the FBI is an agency (or component) of DOJ.

The strategy and HSPDs did not identify multiple leads on any of the five Intelligence and Warning initiatives (see table 7). In addition, these strategic documents clearly named all leads. DHS is named as a clear lead on three Intelligence and Warning initiatives; DOJ is identified as a clear lead on one initiative.

## Fiscal Year 2004 Implementation of the Initiatives

In fiscal year 2004, implementation activity occurred with respect to each of the five Intelligence and Warning initiatives (see table 7). DHS implemented activity in each of the three initiatives for which it was identified as a lead. DOJ implemented activity in the one initiative for which it was named as the lead (enhancing the analytic capabilities of the FBI).

Additionally, several of the departments under review implemented multiple Intelligence and Warning initiative activities for which they were not identified as a lead. During fiscal year 2004, DOE cited implementation activities in four of the five Intelligence and Warning initiatives for which it did not have a lead (prior to fiscal year 2004, it cited implementation activity with respect to three of the five initiatives.) DOD cited fiscal year 2004 implementation activities in 3 of 5 initiatives for which it did not have a lead. DHS cited planning and implementation activities during fiscal year 2004 on the one initiative for which it did not have lead responsibilities; and State cited both prior implementation and 2004 implementation activity on the one initiative for it was not cited as a lead in the strategy or HSPDs.

## Challenges in Intelligence and Warning

With the element of surprise on their side, terrorists have the potential to do massive damage to an unwitting and unprepared target. It therefore follows that the United States must take appropriate action to develop and implement an effective Intelligence and Warning system that is capable of detecting planned terrorist activity, so that proper preemptive, preventive, and protective action can be taken. Our recent work in the Intelligence and Warning mission area has identified a number of challenges. These challenges include enhancing the analytical capabilities of the FBI, improving the coordination and mechanisms for sharing intelligence information across levels of government and the private sector, consolidating terrorist watch lists, and strengthening the homeland security advisory system.

## Enhancing the FBI's Analytical Capabilities

The strategy has an initiative to enhance the FBI's analytic capabilities in order to address the agency's top priority—preventing terrorist attacks. The FBI is, therefore, "creating an analytical capability that can combine lawfully obtained domestic information with information lawfully derived from investigations, thus facilitating prompt investigation of possible terrorist activity within the United States." To accomplish this, the FBI has changed its priorities and accelerated modernization of its information technology (IT) systems. However, we reported in September 2003 that the FBI will be facing a number of challenges as it begins this modernization without having yet developed a modernization blueprint, commonly referred to as an enterprise architecture (a plan that defines how an organization operates today, intends to operate tomorrow, and intends to invest in IT systems to transition to this future state).[4] Architectures are essential to effectively managing such complex endeavors and are recognized as hallmarks of successful public and private organizations. The challenge for the FBI will be to make architecture development an institutional management priority; until this is accomplished and the architecture is developed and implemented, the FBI faces the challenge of ensuring systems currently being developed and deployed will be consistent with the yet-to-be-developed architecture. Our research and experience at federal agencies has shown that attempting a major modernization effort without a well-defined and enforceable architecture results in systems that are duplicative and not well integrated, are unnecessarily costly to operate and maintain, and do not effectively optimize mission performance. Additional challenges related to the FBI's transformation are contained in appendix IV, on domestic counterterrorism. The Bremer, Hart-Rudman, Gilmore, and 9/11 Commissions all made recommendations related to this challenge.

## Improving Intelligence Information Sharing

According to the strategy, "homeland security intelligence and information must be fed instantaneously into the Nation's domestic anti-terrorism efforts, and "this effort must be structured to provide all pertinent homeland security intelligence and law enforcement information—from all relevant sectors including state and local law enforcement as well as federal agencies—to those able to take preventive or protective action." Since September 11, federal, state, and local governments have established initiatives to meet the challenge of sharing information to prevent

[4]See GAO, *Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*, GAO-03-959 (Washington, D.C.: Sept. 25, 2003).

terrorism. DHS has initiatives under way to enhance information sharing (including the development of a homeland security enterprise architecture to integrate sharing among federal, state, and local authorities). In addition, the FBI increased the number of its Joint Terrorism Task Forces, the Defense Intelligence Agency (DIA) entered into an information-sharing partnership with the state of California and the city of New York; and Massachusetts has established an antiterrorism network of state, local, and federal agencies. However, our August 2003 report[5] noted that these initiatives, while beneficial for the partners, presented challenges because they (1) were not well coordinated, (2) rsked limiting participants' access to information, and (3) potentially duplicated the efforts of some key agencies at each level of government. We also found that despite various legislation, strategies, and initiatives, federal agencies, states, and cities did not consider the information sharing process to be effective. For example, information on threats, methods, and techniques of terrorists was not routinely shared, and the information that was shared was not perceived as timely, accurate, or relevant. Additionally, federal agencies were challenged by the inability of state or city governments to properly handle classified information and their lack of security clearances. The Gilmore and 9/11 Commissions made recommendations related to this challenge.

## Better Dissemination of Threat Information to the Private Sector

The strategy discusses the need for threat-vulnerability integration, providing that "mapping terrorist threats and capabilities—both current and future—against specific facility and sectoral vulnerabilities will enable authorities to determine which organizations pose the greatest threat and which facilities are most at risk." However, in a March 2003 report we noted that one of the nation's challenges is to develop and implement methods for effectively sharing information between government and the private sector.[6] For example, officials in several commercial industries have said that they need better threat information from law enforcement agencies, as well as better coordination among agencies providing threat information. Specifically, these officials stated that they did not receive

[5]See GAO, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760 (Washington, D.C.: Aug. 27, 2003).

[6]See GAO, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-439 (Washington, D.C.: Mar. 14, 2003); *Drinking Water: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security*, GAO-04-29 (Washington, D.C.: Oct. 31, 2003).

sufficient specific threat information, and frequently received threat information from multiple government agencies. Similarly, DOJ observed that chemical facilities need more specific information about potential threats in order to design their security systems and protocols. Threat information also forms the foundations for some of the tools available to industry to assess facility vulnerabilities. Threat information is the foundation for hypothesizing about threat scenarios, which form the basis for determining site vulnerabilities. In reviewing security considerations involving commercial seaports, we found that similar challenges existed. Specifically, on the basis of visits to several of the commercial seaports designated by DOD as critical for use by the military for overseas deployments, we reported in October 2002 that although the organizations responsible for seaport security increased emphasis on security planning since September 11, there remained no single mechanism to analyze, coordinate, and disseminate threat information on a routine basis on the broad range of threats at each port.[7] Most threat information was coordinated on an informal basis, increasing the risk that threats—both traditional and nontraditional ones—may not be recognized or that threat information may not be communicated in a timely manner to all relevant organizations, including private sector organizations, at the ports. The Gilmore and 9/11 Commissions made recommendations related to this challenge.

## Consolidating Terrorist Watch Lists

The strategy recognizes the need for "fully accessible sources of information related to suspected terrorists" through the establishment of a consolidated terrorism watch list. In April 2003 we reported that changing the federal government's diffused and nonstandard approach to developing and using terrorist watch lists—which are essential tools for performing, among other things, the nation's border security mission—involve addressing key management, technical, and legal challenges.[8] One of these challenges involves defining and implementing a new approach that overcomes individual agencies' unique culture and mission requirements. For example, a key reason for the varying extent to which watch list sharing is done involves cultural differences among the government and private sector agencies involved in securing our borders.

[7]See GAO, *Combating Terrorism: Actions Needed to Improve Force Protection for DOD Deployments through Domestic Seaports*, GAO-03-15 (Washington, D.C.: Oct. 22, 2002).

[8]See GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322 (Washington, D.C.: Apr. 15, 2003).

Another challenge to be overcome involves the tendency of the watch lists to have overlapping but not identical sets of data, which makes their consolidation difficult. Additionally, the extent to which such sharing is accomplished electronically is constrained by fundamental differences in the watch lists' systems architecture (that is, the hardware, software, network, and data characteristics of the systems). Finally, while legal requirements have historically been another challenge to sharing, recent legislation has begun to address this barrier. For example, Congress passed the USA PATRIOT ACT, which has significantly changed the legal framework for information sharing when fully implemented, it should diminish the effect of existing legal barriers.[9] The 9/11 Commission made recommendations related to this challenge.

## Strengthening the Homeland Security Advisory System

The strategy calls for the implementation of the Homeland Security Advisory System as a means of disseminating information regarding the risk of terrorist acts to federal, state, and local authorities; the private sector; and the American people. Utilizing five color-coded threat levels, the system was established by HSPD-3 in March 2002. However, in a March 2004 testimony, we reported that DHS faces challenges in strengthening the advisory system and keeping it relevant and viable. For example, the system has generated questions concerning the quality and timeliness of the threat information being disseminated.[10] Specifically, DHS had not yet officially documented communication protocols for threat information and guidance to federal agencies and states, with the result that some federal agencies and states first learn about changes in the national threat level from the media. An additional challenge relates to the comprehensiveness of information provided with regard to actions to be taken in response to changes in the threat level. For example, public warnings did not include guidance on actions to be taken in response to a specific threat. Moreover, federal agencies responding to our inquiries indicated that an additional challenge involves their inability to determine appropriate protective measures to be implemented because of a lack of specific threat information. For example, federal agencies indicated to us that, particularly, region-, sector-, site-, or event-specific threat information—to the extent that it is available—would be helpful. Since the time of our

[9]Pub. L. 107-56.

[10]See GAO, *Homeland Security: Risk Communication Principles May Assist in Refinement of the Homeland Security Advisory System*, GAO-04-538T (Washington, D.C.: Mar. 16, 2004).

report, DHS has provided more specific warnings by both sector (e.g., the financial sector) and location (e.g., New York and Washington, D.C.). The Gilmore Commission made recommendations related to this challenge.

# Appendix III: Border and Transportation Security

This appendix sets forth the definition and major initiatives of the Border and Transportation Security mission area and discusses the agencies with major roles, their funding, the alignment of their strategic plans and implementation activities with the major initiatives, and a summary of the key challenges faced by the nation. This appendix presents baseline information that can be used by Congress to provide oversight and track accountability for the initiatives in the Border and Transportation Security mission area.

## Definition and Major Initiatives

The *National Strategy for Homeland Security* categorizes homeland security activities into six critical mission areas, the second of which is Border and Transportation Security. This mission area includes programs designed to fully integrate homeland security measures into existing domestic transportation systems and focuses on promoting the efficient and reliable flow of people, goods, and services across borders, while preventing terrorists from using transportation conveyances or systems to deliver implements of destruction. Activities in this mission area often dovetail into domestic counterterrorism as agencies take law enforcement action to address potential threats to the homeland that may originate along our borders or in our transportation systems. Also, because transportation is a critical infrastructure sector, this mission area is also closely related to the critical infrastructure protection mission area. For example, homeland security actions at seaports would involve activities in both mission areas.[1] Figure 5 shows an example of the type of activities found in the Border and Transportation Security mission area.

The strategy identifies the following major initiatives in the border and transportation mission area:

- ensuring accountability in border and transportation security,
- creating smart borders,
- increasing the security of international shipping containers,
- implementing the Aviation and Transportation Security Act of 2001,
- recapitalizing the U.S. Coast Guard, and
- reforming immigration services.

[1]This definition is from OMB's *2003 Report to Congress on Combating Terrorism* (Washington, D.C.: Sept. 2003).

**Figure 5: U.S. Customs and Border Patrol Marine Officers on the Waters of the Rio Grande, along the United States and Mexico Border**

Source: U.S. Customs and Border Patrol.

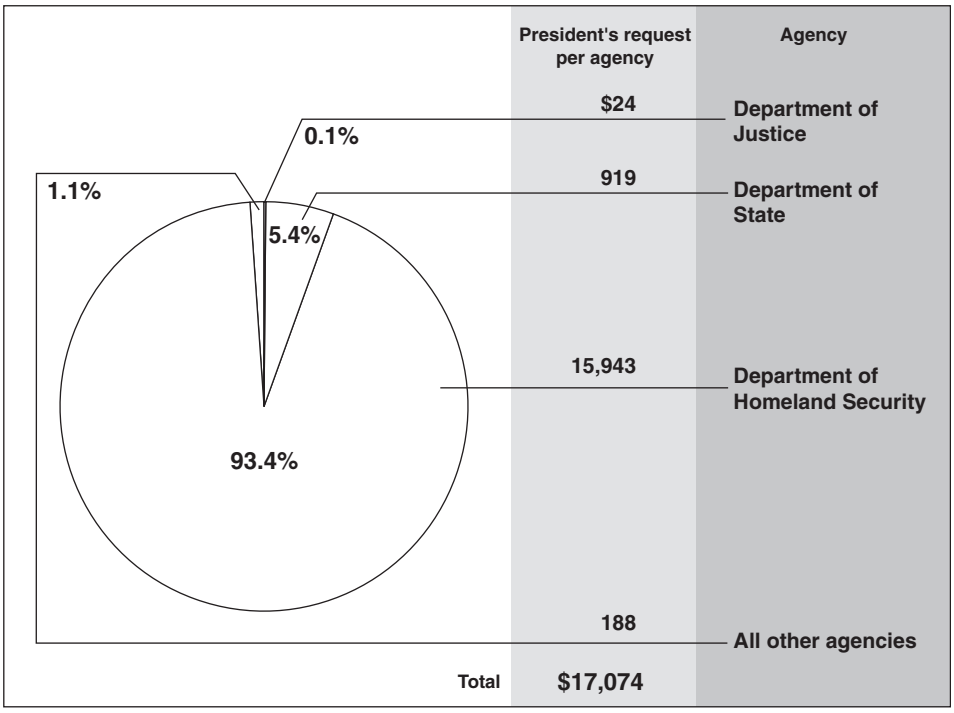
## Agencies with Major Roles in Border and Transportation Security

Of the six agencies under review, DHS and State have major roles in Border and Transportation Security. Within DHS, the U.S. Customs and Border Protection (CBP) conducts inspections at ports of entry to detect and prevent people and goods from entering the country illegally, while the Bureau of Immigration and Customs Enforcement (ICE) investigates and enforces laws against the unlawful presence of people and goods in the country; the Transportation Security Administration (TSA) performs some aviation security activities, while overseeing others, and coordinates the development of security measures for nonaviation modes of transportation; and the U.S. Coast Guard leads security activities at the nation's ports. State plays a role in this mission area through its administration of the visa program to ensure against travel into the United States by terrorists or others whose presence may undermine U.S. national security. Although not one of six agencies we reviewed, the Department of Agriculture (USDA) also has a role in border and transportation security. Specifically, USDA's Animal and Plant Health Inspection Service (APHIS) performs agricultural quarantine activities and risk analysis at U.S. ports of entry.

OMB reported that the total fiscal year 2005 funding request for border and transportation security is $17 billion, with the majority of this going to DHS (almost $16 billion, or 93 percent), largely for CBP, TSA, and the Coast Guard. Other DHS bureaus, as well as other agencies—such as USDA and State—have significant funding in this mission area as well.[2] Figure 6 summarizes the fiscal year 2005 budget request for the border and transportation security mission area by agency.

[2]OMB, *Analytical Perspectives*, *Budget of the United States Government*, *Fiscal Year 2005* (Washington, D.C.: Feb. 2004).

**Figure 6: Proposed Fiscal Year 2005 Homeland Security Funding for Border & Transportation Security**




Source: GAO, based on OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005.*

Notes: Budget authority in millions of dollars.

"All other agencies" includes USDA ($169 million) and the Department of Transportation ($19 million).

OMB's reported data do not include funding for three departments that have activities under way in this mission area. These departments—DOD, HHS, and DOE—have either planning or implementation activity on specific initiatives, as discussed in the next section of this appendix. On the basis of previous work, we have noted several qualifications to OMB's figures to explain this discrepancy.[3] According to OMB officials, there is not always a clear distinction between homeland security activities and other related activities. OMB staff must make judgment calls about how to characterize funding by mission areas. For example, some homeland security activities have multiple purposes, and funding for these activities is comingled in accounts that can cover multiple mission areas. In

[3]See GAO-03-170.

addition, some of the departments' activities, such as planning, coordination, or providing advice may support Border and Transportation Security activities but are not included in the amounts shown.

## Alignment of Department Activities with the Major Initiatives

This section provides more detailed information about the Border and Transportation Security mission area initiatives and the departments involved in conducting activities related to these initiatives. This includes a discussion of specific departmental planning and implementation activities, lead agency designations, and implementation activities in fiscal year 2004, with respect to each initiative. The data are summarized in table 8.

**Table 8: Detailed Department Leadership and Planning/Implementation Activities in the Border and Transportation Mission Area's Six Initiatives**

| | DHS | | | DOJ | | | DOD | | | HHS | | | State | | | DOE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 |
| **Border and transportation security** | | | | | | | | | | | | | | | | | | |
| (1) Ensure accountability in border and transportation security | ● | ● | ● | | | | ● | ● | ● | | ● | ● | ● | ● | ● | ● | | |
| (2) Create "smart borders" | ● | ● | ● | ● | ● | | | | | | ● | ● | ● | ● | ● | | | |
| (3) Increase the security of international shipping containers | ● | ● | ● | | | | ● | | ● | | | | ● | ● | ● | ● | | ● |
| (4) Implement the Aviation and Transportation Security Act of 2001 | | ● | ● | | | | | ● | ● | | | | | | | | | |
| (5) Recapitalize the U.S. Coast Guard | ● | ● | ● | | | | ● | ● | | | | | | | | | | |
| (6) Reform immigration services | ● | ● | ● | ● | ● | | | | | | | | ● | ● | ● | | | |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Department IMPLICITLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

PI = Prior implementation to fiscal year 2004
RP = Recent planning
04 = Fiscal year 2004 implementation

Source: GAO.

## Summary of Departmental Activities on the Initiatives

All six Border and Transportation Security initiatives are being addressed in at least two of the key departments' planning and implementation activities (see table 8). At least three departments cited activity in four of the six initiatives. For example, DHS, DOD, State, and DOE implemented

shipping container security initiative (CSI) activities in fiscal year 2004. DHS deployed Customs and Border Protection officers to Malaysia to conduct CSI activity; DOD provided an intelligence perspective on container and port security vulnerabilities, aiding in the development and deployment of technologies; State engaged in diplomatic efforts with additional countries to conclude further CSI agreements; and DOE worked with Lithuania to install nuclear detection equipment at the Vilnius Airport, as well as other airports and other locations in other foreign countries. Additionally, DHS, HHS, and State demonstrated implementation activities in fiscal year 2004 with respect to creating smart borders. DHS developed, acquired, and deployed biometrically enabled, travel document reader technology, at air, sea, and land ports of entry; the Food and Drug Administration within HHS established guidance requiring the registration of domestic and foreign facilities that manufacture, process or hold food for consumption in the United States; and State deployed biometric collection capability to consular posts worldwide.

All six departments have been engaged in Border and Transportation Security initiatives.

While we have identified department activities relates to these initiatives, we did not determine the quality, status, or progress of such activities with respect to stated goals or targets within this mission area.

## Identification of Lead Agencies on the Initiatives

For all six initiatives, a lead agency is identified either in the strategy or HSPDs. As shown in table 8, DHS is the lead on the most initiatives in the mission area—six of six initiatives. It is understandable that DHS would be the department with the most initiative leads, given that the initiatives (a) emphasize DHS's twin goals of preventing terrorist attacks and reducing border vulnerability; and (b) reflect a transfer of the Customs Service, Immigration and Naturalization Service, and Coast Guard to DHS. State is also identified as a lead on the initiative to create smart borders. Given the initiative's emphasis on visa issuance and consular office participation in detecting potential terrorists, it seems appropriate that State would be identified in a leadership capacity. DOJ had been identified as a lead agency with respect to two initiatives, creating smart borders and guarding America's critical infrastructure and key assets against "inside" threats. However, given the transfer of the Immigration and Naturalization Service and the National Infrastructure Protection Center programs to the Department of Homeland Security, DOJ officials indicated the department no longer serves as the lead on these two initiatives.

Creating smart borders is the only initiative for which there are multiple leads in the Border and Transportation Security area (see table 8). The two department leads in this initiative are DHS and State. Additionally, departmental documents show that DHS is a clear lead on two initiatives and an implied lead on three initiatives. State is a clear lead on its single initiative.

## Fiscal Year 2004 Implementation of the Initiatives

In fiscal year 2004 implementation activity occurred with respect to all six Border and Transportation Security initiatives (see table 8). DHS implemented activity in all five initiatives for which it was identified as a lead. State implemented activity in the one initiative where it was designated a lead.

Additionally, several of the departments under review implemented multiple Border and Transportation Security initiatives for which they were not identified as a lead agency in the strategy and HSPD. During fiscal year 2004, DOD cited implementation activities in three initiatives for which it did not have any lead responsibilities (prior to fiscal year 2004, DOD cited planning/implementation activity with respect to four of the six initiatives). State cited fiscal year 2004 and prior year implementation activity on three initiatives, for which it was not identified as the lead; HHS cited 2004 implementation activity on two initiatives without lead responsibilities; and DOE cited both 2004 and prior implementation with respect to one initiative.

DOJ has not demonstrated fiscal year implementation activity in any initiative within this critical mission area; a DOJ official indicated that this is due to program transfers. In accordance with the Homeland Security Act of 2002, DOJ transferred its Immigration and Naturalization Service programs to DHS.

# Challenges in Border and Transportation Security

The strategy calls for ensuring the "efficient and reliable flow of people, goods, and services across borders, while preventing terrorists from using transportation conveyances or systems to deliver implements of destruction." Our recent work in the Border and Transportation Security mission area has identified a number of challenges. Among the challenges faced is striking a balance between increased border security with concerns for facilitating legitimate travel and the flow of goods, the need to address problems associated with processing people at the nation's ports of entry, training border security personnel to detect counterfeit documents and fictitious identities, determining the proper role for

biometric technologies for security applications, developing a clear and comprehensive visa process, and improving the management of key programs. The challenges that we have identified in ensuring that our transportation system is secure include implementing an effective system to prescreen airline passengers; achieving and sustaining improvements in airline passenger, baggage, and cargo screening; strengthening perimeter security and access controls at airports; adequately addressing rail and mass transit security issues; and recapitalizing the U.S. Coast Guard.

# Border Security

## Balancing Security Concerns with Economic Needs

The strategy recognizes the long-standing challenge of balancing our nation's security and commercial needs and states that the "efficient flow of people, goods, and conveyances engaged in legitimate economic and social activities" must not be impeded. Primary responsibility for ensuring the balance between security and commercial needs falls on DHS's CBP. In a June 2003 testimony, we reported that CBP faces many challenges in trying to accomplish its mission.[4] Concerning the efficient flow of people, challenges include detecting false admissibility documents, unifying and enhancing inspector training, providing timely intelligence to the field, and successfully implementing the new entry-exit system. With respect to cargo, CBP has attempted to select and inspect the highest-risk incoming cargo while enabling legitimate cargo to be cleared in a timely manner. These efforts pose a range of challenges, from the availability of threat assessments and actionable intelligence to the capability of nonintrusive inspection technology to detect potentially harmful contraband. Additional challenges faced by CBP include the need to improve its trade compliance program and to successfully implement its new trade-processing information system. The Gilmore, Hart-Rudman, and 9/11 Commissions made recommendations related to this challenge.

## Effectively Processing People at Land Ports of Entry

The strategy calls for DHS to "verify and process the entry of people in order to prevent the entrance of contraband, unauthorized aliens, and potential terrorists." However, in a June 2003 testimony and an August

[4]See GAO, *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).

2003 report, we indicated that CBP, the entity within DHS that is responsible for carrying out this task, faces several challenges at land ports of entry related to the determination of traveler admissibility and other vulnerabilities in the inspection process.[5] In 2003, we testified that CBP inspectors faced a variety of challenges at the ports, including the need to make quick decisions on whether to immediately admit a traveler into the country or refer the traveler for more intensive inspection. This task is made more challenging because (1) United States and certain Canadian citizens may enter this country without presenting a travel document if they make an oral claim of citizenship that satisfies the inspector and (2) travelers who are required to show an identity document can present a variety of documents, some of which can be easily counterfeited. In fact, in October 2003, we testified about the challenges posed by identity fraud and how counterfeit identification can be easily produced and used to create fraudulent identities.[6] We also identified other challenges for CBP at the borders, including ensuring that inspectors are adequately trained in conducting inspections and detecting fraudulent documents and challenges regarding the collection, analysis, and use of intelligence information in the field. The Gilmore, Hart-Rudman, and 9/11 Commissions made recommendations related to this challenge.

## Effectively Employing Biometric Technologies

The strategy states that the "United States will require visitors to present travel documentation that includes biometric indicators." However, in a November 2002 report and in March and September 2003 testimonies, we reported that challenges exist in determining the proper role of biometric technologies for security applications.[7] The first challenge involves recognizing that the use of biometric technology not a panacea for the border security problem. Instead, it is just a piece of the overall decision support system that helps determine whether or not a person is allowed to enter the United States. For example, while biometrics may be useful in reducing document fraud, it may not have much effect on the ability of people to enter the United States through other than official ports of entry.

[5]See GAO, *Land Border Points of Entry: Vulnerabilities and Inefficiencies in the Inspections Process*, GAO-03-1084R (Washington, D.C.: Aug. 18, 2003); and GAO-03-902T.

[6]See GAO, *Counterfeit Identification Raises Homeland Security Concerns*, GAO-04-133T (Washington, D.C.: Oct. 1, 2003).

[7]See GAO, *Information Security: Challenges in Using Biometrics*, GAO-03-1137T (Washington, D.C.: Sept. 9, 2003); *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002); and *Border Security: Challenges in Implementing Border Technology*, GAO-03-546T (Washington, D.C.: Mar. 12, 2003).

Another major challenge involves questions regarding the technical and operational effectiveness of biometric technologies in applications as large as border control. Additional challenges to be addressed include determining (1) the system's effect on existing border control procedures and people; (2) the costs and benefits of the system, including secondary costs resulting from changes in processes or personnel to accommodate the biometrics; and (3) the system's effect on privacy, convenience, the economy, and relations with other countries. The 9/11 Commission made recommendations related to this challenge.

## Deploying Effective Technologies for the Detection of Weapons of Mass Destruction

The strategy states that the nation will "develop and deploy non-intrusive inspection technologies to ensure rapid and more thorough screening of goods and conveyances." We reported in October 2002,[8] however, that challenges exist with regard to the acquisition and deployment of radiation detection equipment. In particular, we have concerns that DHS has not yet deployed the best available technologies for detecting radioactive and nuclear materials at U.S. border crossings and ports of entry. Specifically, we have found that CBP's primary radiation detection equipment—radiation pagers—have certain limitations and may be inappropriate for the task. For example, according to U.S. radiation detection vendors and DOE laboratory specialists, pagers are more effectively used in conjunction with other radiation detection equipment, such as portal monitors and radio isotope identifiers. A further challenge is the need for a comprehensive plan for installing and using radiation detection equipment at all U.S. border crossings and ports of entry. A comprehensive plan would address, among other things, vulnerabilities and risks; identify the complement of radiation detection equipment that should be used at each type of border entry point—air, rail, land, and sea—and whether the equipment could be immediately deployed; identify longer-term radiation detection needs; and develop measures to ensure that the equipment is adequately maintained. Finally, there is a challenge that goes beyond simply deploying equipment—personnel must be effectively trained in radiation science, the proper use of the detection equipment, and how to identify and respond to alarms.

## Using Visas as an Antiterrorism Tool

The strategy calls on DHS to "build an immigration services organization that administers immigration laws in an efficient, expeditious, fair, and

[8]See GAO, *Customs Service: Acquisition and Deployment of Radiation Detection Equipment*, GAO-03-235T (Washington, D.C.: Oct. 17, 2002).

humane manner" while ensuring "that foreign visitors comply with entry conditions." In carrying out its goal of reforming our nation's immigration services, DHS faces a number of challenges.

The first involves the development of a clear policy on how to balance national security concerns with the desire to facilitate legitimate travel when issuing visas. Specifically, we reported in October 2002 that this process should be strengthened for use as an antiterrorism tool.[9] We also identified the need for more coordination and information sharing to realize the full potential of the visa process. In addition, there is a need for more human resources and more training for consular officers.

An additional challenge concerns the lack of a governmentwide policy on the interagency visa revocation process. This process is an important tool for preventing potential terrorists from entering the country and identifying potential terrorists who have already entered. However, we testified in June 2003 that weaknesses in the process we first identified in June 2003 have not been eliminated, especially those related to the timely transmission of information among government agencies.[10] Our review of visas revoked for terrorism concerns from October through December 2002 showed that delays occurred in screening names of suspected terrorists for visa holders, transmitting recommendations to revoke individuals' visas, revoking visas after receiving recommendations to do so, and posting lookouts. We also found delays in notifying immigration officials of the need to investigate individuals with revoked visas who may be in the country and in initiating field investigations of those individuals. Finally, challenges exist because of unresolved legal and policy issues regarding the removal of individuals from the United States based solely on their visa revocation. For example, there needs to be clear, comprehensive policies governing visa processes and procedures so that all agencies involved agree on the level of security screening for foreign nationals both at our consulates abroad and at ports of entry.

A third challenge concerns the Visa Waiver Program. This involves discussing the process established by the Departments of Justice and State for determining whether a country is eligible to participate in the program.

[9]See GAO, *Border Security: Visa Process Should Be Strengthened as an Antiterrorism Tool*, GAO-03-132NI (Washington, D.C.: Oct. 21, 2002).

[10]See GAO, *Border Security: New Policies and Procedures Are Needed to Fill Gaps in the Visa Revocation Process*, GAO-03-1013T (Washington, D.C.: June 18, 2003).

For example, one of the laws passed since the terrorist attacks of September 11, requires participating countries to issue passports that contain biometric identifiers, such as fingerprints. However, it is unclear whether these requirements will be fully implemented by the deadlines called for in the law. In our November 2002 report,[11] we also pointed out that the national security challenges created by eliminating the Visa Waiver Program are difficult to determine, but that doing so could affect U.S. relations with other countries, U.S. tourism, and State Department resources abroad. For example, if the program were eliminated, we estimated that the department's initial costs to process the additional workload would range between $739 million and $1.28 billion, and annual recurring costs would likely range between $522 million and $810 million. It could take 2 to 4 years or longer to put the necessary people and facilities in place to handle the increased workload, according to State officials.

An additional challenge involves reducing the time taken to adjudicate visas for science students and scholars. Specifically, we reported in February 2004[12] that the time it takes to adjudicate a visa for a science student or scholar depends largely on whether an applicant must undergo a security check that is designed to protect against sensitive technology transfers. We took a random sample of these security checks for science students and scholars sent from posts abroad between April and June 2003 and found it took an average of 67 days for security checks to be processed and for State to notify the post. Officials from the State Department and FBI acknowledged there have been lengthy waits, but reported having measures under way that they believe will improve the process. However, additional challenges remain, such as interoperability issues between State's and FBI's computer systems.

Finally, a challenge exists in balancing national security concerns with the expeditious processing of visa applications. Specifically, we reviewed[13] the visa operations at U.S. posts in Canada and provided information on the perceptions of consular staff that adjudicate U.S. visas regarding the

[11]See GAO, *Border Security: Implications of Eliminating the Visa Waiver Program*, GAO-03-38 (Washington, D.C.: Nov. 22, 2002).

[12]See GAO, *Border Security: Improvements Needed to Reduce Time Taken to Adjudicate Visas for Science Students and Scholars*, GAO-04-371 (Washington, D.C.: Feb. 26, 2004).

[13]See GAO, *Visa Operations at U.S. Posts in Canada*, GAO-04-708R (Washington, D.C.: May 18, 2004).

importance of national security in the visa process, including impediments that could interfere with efforts to make security a top priority in visa processing. Consular officers and managers at U.S. posts in Canada said that despite rising workloads and increasingly labor-intensive visa-processing requirements, they were placing an emphasis on security in visa operations. Some officers reported that new post-September 11 processing requirements for visas could reduce the time available for face-to-face interviews. While most officers believed that they had enough time to screen applicants carefully for possible security risks, some of the newer officers at posts in Canada expressed concern about their ability to remain vigilant if the workload increased.

The Bremer and 9/11 Commissions made recommendations related to the challenges found in this section.

## Improving the US-VISIT Program

Integral to the effort to reform immigration services and the strategy's call for a "border of the future," is the implementation of the United States Visitor and Immigrant Status Indicator (US-VISIT) program, which is designed to collect, maintain, and share information, including biometric identifiers, on selected nationals who travel to the United States. We testified in March 2004[14] that this implementation is challenging because of the type of program it is and the way it is being managed. US-VISIT is to perform a critical, multifaceted mission, its scope is large and complex, it must meet a demanding implementation schedule, and its potential cost is enormous. One critical aspect of the program's mission is to prevent the entry of persons who pose a threat to the United States. DHS estimated that the program would cost $7.2 billion through fiscal year 2014, but this estimate did not include all costs and underestimated some others. In addition, several factors related to the program's management increase the risk of not delivering mission value commensurate with costs or not delivering defined program capabilities on time and within budget. Also, the requirements for interim facilities at high-volume land ports of entry are not only demanding, they are based on assumptions that, if altered, could significantly affect facility plans. Despite these challenges, the first increment was deployed at the beginning of 2004. DHS's fiscal year 2004 US-VISIT expenditure plan and related documentation at least partially satisfies all conditions imposed by Congress. US-VISIT largely met its

[14]See GAO, *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed*, GAO-04-569T (Washington, D.C.: Mar. 18, 2004).

commitments for implementing an initial operating capability in early January 2004, including the deployment of entry capability to 115 air and 14 seaports of entry. However, challenges remain because DHS has not employed rigorous, disciplined management controls typically associated with successful programs. More specifically, testing of the initial phase of the implemented system was not well managed and was completed after the system became operational. In addition, multiple test plans were developed during testing, and only the final test plan, completed after testing, included all required content. Such controls, while significant for the initial phases of US-VISIT, are even more critical for the later phases, as the size and complexity of the program will only increase. Finally, as we reported in May 2004,[15] DHS's plans for future US-VISIT resource needs at the land ports of entry are based on questionable assumptions, making future resource needs uncertain. The 9/11 Commission made recommendations related to this challenge.

# Transportation Security

## Effectively Prescreening Aviation Passengers

Developing an effective system to prescreen passengers before they even arrive at the airport is one of the challenges alluded to in the strategy's discussion of the implementation of the Aviation and Transportation Security Act (ATSA) of 2001. DHS's solution to this challenge was the development of the Computer-Assisted Passenger Prescreening Program (CAPPS II), which was designed to identify passengers requiring additional security attention. As we said in a February 2004 report and in a March 2004 testimony,[16] key activities in the development of this program have been delayed or not addressed. We also identified three additional challenges TSA faces that may impede the success of CAPPS II. These challenges are developing the international cooperation needed to obtain passenger data, managing the possible expansion of the program's mission beyond its original purpose, and ensuring that identity theft cannot be

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

[16]See GAO, *Aviation Security: Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System*, GAO-04-504T (Washington, D.C.: Mar. 17, 2004); and *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (Washington, D.C.: Feb. 12, 2004).

used to negate the security benefits of the system. Recently the Transportation Security Administration scrapped the CAPPS II program and created a follow-on program called Secure Flight, which could face many of the same challenges we identified. The 9/11 Commission made recommendations related to this challenge.

## Improving Airline Passenger and Baggage Screening

Another of the challenges alluded to in the strategy's discussion of ATSA is the effective and efficient screening of passengers and baggage. This has been a long-standing concern, and although significant actions have been taken, we testified in February and March 2004 that challenges in achieving and sustaining improvements remain.[17] For example, while TSA met its mandate to establish a federal screener workforce by November 2002, it continues to face challenges in hiring and deploying passenger and baggage screeners. Additionally, while TSA is making progress in measuring the performance of passenger screeners, it has collected limited performance data related to its baggage screening operations. Moreover, testing of screeners has identified weaknesses in their ability to detect threat objects, while essential training is hampered by staffing shortages and a lack of adequate technical capability to access online training programs. Still another challenge involves deploying and leveraging screening equipment and technologies. For example, TSA continues to face operational and funding challenges in its efforts to achieve a mandate to screen all baggage using explosive detection systems. The 9/11 Commission made recommendations related to this challenge.

## Strengthening Airport Perimeter Security and Access Controls

Another key requirement of ATSA, as discussed in the strategy, is the "protection of critical infrastructure assets," including airports. In June 2004[18] we reported that while TSA has begun evaluating the security of airport perimeters and access controls, the agency has not yet determined how the results will be used to address the challenges faced. Specifically, these challenges include addressing concerns with perimeter and access control security that have been raised in compliance inspections and

[17]GAO, *Aviation Security: Challenges Exist in Stabilizing and Enhancing Passenger and Baggage Screening Operations*, GAO-04-440T (Washington, D.C.: Feb. 12, 2004); and *Aviation Security: Private Screening Contractors Have Little Flexibility to Implement Innovative Approaches*, GAO-04-505T (Washington, D.C.: Apr. 22, 2004).

[18]See GAO, *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).

vulnerability assessments; setting priorities for funding airport security needs, developing a plan for implementing new technologies to meet security needs, and implementing certain mandated actions to reduce the security threats posed by airport workers.

## Countering Threats Posed by Hand-Held Missiles

Another consideration for ensuring the security of our aviation system involves the issue of aircraft protection, specifically countering the threats posed by Man-Portable Air Defense Systems (MANPADS). These hand-held missile systems have been used by terrorists against commercial aircraft.

In January 2004, we reported[19] that DHS faces significant challenges in adapting a military counter-MANPADS system to commercial aircraft, such as establishing system requirements, developing technology and design to sufficient maturity, and setting reliable cost estimates. Our work on the best practices of product developers in government and industry has found that such challenges can be successfully overcome by using a knowledge-based approach.

Additionally, in a May 2004 report,[20] we found that further improvements are needed in U.S. efforts to keep MANPADS out of the hands of terrorists. Although the State Department made important progress in 2003 to control the global proliferation of MANPADS, its ability to assess further progress is limited because multilateral forums have no mechanisms to monitor members' implementation of commitments. DOD has sold thousands of Stinger missiles (a U.S. MANPADS) to 17 countries and Taiwan, but DOD agencies responsible for end-use monitoring are not required to maintain records on the number and destination of Stinger sales. In addition, DOD officials overseas use inconsistent practices when inspecting Stinger inventories because DOD lacks procedures for conducting these inspections. For example, DOD has no requirements for DOD organizations responsible for end-use monitoring to keep records on the number and destinations of these Stingers.

[19]See GAO, *The Department of Homeland Security Needs to Fully Adopt a Knowledge-based Approach to Its Counter-MANPADS Development Program*, GAO-04-341R (Washington, D.C.: Jan. 30, 2004).

[20]See GAO, *Nonproliferation: Further Improvements Needed in U.S. Efforts to Counter Treats from Man-Portable Air Defense Systems*, GAO-04-519 (Washington, D.C.: May 12, 2004).

## Effectively Addressing Rail and Mass Transit Security Issues

The strategy recognizes "the importance of security for all forms of transportation." As we testified[21] in March and September 2003, certain characteristics of mass transit systems make them inherently vulnerable to terrorist attacks and a challenge to secure. By design, mass transit systems are open (i.e., have multiple access points and, in some case, no barriers) so that they can move large numbers of people quickly. In contrast, the aviation system is housed in closed and controlled locations with few entry points. The openness of mass transit systems can leave them vulnerable because transit officials cannot monitor or control who enters or leaves the systems. In addition, other characteristics of some transit systems—high ridership, expensive infrastructure, economic importance, and location (e.g., large metropolitan areas or tourist destinations)—also make them attractive targets because of the potential for mass casualties and economic damage. Moreover, some of these same characteristics make mass transit systems difficult to secure. For example, the number of riders that pass through a mass transit system—especially during peak hours—makes some security measures, such as metal detectors, impractical. In addition, the multiple access points along extended routes make the costs of securing each location prohibitive.

Further complicating transit security is the challenge faced by transit agencies in balancing security concerns with accessibility, convenience, and affordability. Because transit riders often could choose another means of transportation, such as personal automobile, transit agencies must compete for riders. To remain competitive, transit agencies must offer convenient, inexpensive, and high-quality service. Therefore, security measures that limit accessibility, cause delays, increase fares, or otherwise cause inconvenience could push people away from mass transit and back into their cars.

The size and diversity of the freight rail system make it a challenge to adequately secure. The freight rail system's extensive infrastructure crisscrosses the nation and extends beyond our borders to move millions of tons of freight each day. There are over 100,000 miles of rail in the United States. The extensiveness of the infrastructure creates an infinite number of targets for terrorists. In addition, protecting freight rail assets from attack is made more difficult because of the tremendous variety of

[21]See GAO, *Transportation Security: Post-September 11th Initiatives and Long-Term Challenges*, GAO-03-616T (Washington, D.C.: Mar. 31, 2003), and *Transportation Security: Federal Action Needed to Enhance Security Efforts*, GAO-03-1154T (Washington, D.C.: Sept. 9, 2003).

freight hauled by railroads. For example, railroads carry freight as diverse as dry bulk (grain) and hazardous materials.[22] The transport of hazardous materials is of particular concern because serious incidents involving these materials have the potential to cause widespread disruption or injury. In 2001, over 83 million tons of hazardous materials were shipped by rail in the United States across the rail network, which extends through every major city as well as thousands of small communities. The 9/11 Commission made recommendations related to this challenge.

## Effectively Implementing the Maritime Transportation Security Act

The strategy calls for "targeted improvements in the areas of maritime domain awareness, command and control systems, and shore-side facilities." In response to concerns regarding port security, Congress passed the Maritime Transportation Security Act (MTSA), mandating specific security preparations for America's maritime ports. Passed in November 2002, MTSA imposed an ambitious schedule of requirements on a number of federal agencies. MTSA called for a comprehensive security framework—one that included planning, personnel security, and careful monitoring of vessels and cargo. Agencies responsible for implementing the security provisions of MTSA and have made progress in meeting their requirements. However, in a September 2003 testimony, we identified challenges that merit attention and further oversight.[23]

The main security-related challenge involves the implementation of a vessel identification system. MTSA called for the development of an automatic identification system. Coast Guard implementation calls for a system that would allow port officials and other vessels to determine the identity and position of vessels entering or operating within the harbor area. Such a system would provide an "early warning" of an unidentified vessel or a vessel that was in a location where it should not be. To implement the system effectively, however, requires considerable land-based equipment and other infrastructure that is not currently available in

[22]Federal hazardous material transportation law defines a hazardous material as a substance or material that the Secretary of Transportation has determined is capable of posing an unreasonable risk to health, safety, and property when transported in commerce (49 U.S.C. § 5103). It includes hazardous substances such as ammonia, hazardous wastes from chemical manufacturing processes, and elevated temperature materials such as molten aluminum.

[23]See GAO, *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain*, GAO-03-1155T (Washington, D.C.: Sept. 9, 2003).

many ports. As a result, for the foreseeable future, the system will be available in less than half of the 25 busiest U.S. ports.

Challenges also exist regarding the proposed approach for meeting MTSA's requirement that the Secretary of DHS approve security plans for all vessels operating in U.S. waters. Vessel security plans include taking such steps as responding to assessed vulnerabilities, designating security officers, conducting training and drills, and ensuring that appropriate preventive measures will be taken against security incidents. To implement this MTSA requirement, the Coast Guard has stated, in general, that it is not the Coast Guard's intent to individually approve vessel security plans for foreign vessels. The Coast Guard provides that it will deem a flag-state approval of a vessel security plan to constitute the MTSA-required approval of MTSA vessel security plans. However, MTSA does not mention any role for foreign nations in the required approval of vessel security plans, and some concerns have been raised about the advisability of allowing flag states—some with a history of lax regulation—to ensure the security of vessels traveling to the United States.

Another security-related challenge involves the Coast Guard's efforts to address MTSA's security planning requirements through a series of security assessments of individual ports. Security assessments are intended to be in-depth examinations of security threats, vulnerabilities, consequences, and conditions throughout a port, including not just transportation facilities but also factories and other installations that pose potential security risks. The Coast Guard had begun these assessments before MTSA was passed and decided to continue the process, changing it as needed to meet MTSA planning requirements, which include developing area security plans based on the evaluation of specific facilities throughout the port. Issues were found in the scope and quality of the assessments and their usefulness to port stakeholders. The Gilmore Commission made recommendations related to this challenge.

## Improving Container Cargo Security

The strategy states that "containers are an indispensable but vulnerable link in the chain of global trade" and has an initiative to "increase the security of international shipping containers." As we stated in our July 2003 report,[24] CBP has taken steps to address the challenge of terrorist

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

threats to oceangoing cargo containers through a targeting strategy. CBP faces continuing challenges in targeting containers for inspections. CBP needs upon which to target containers for inspection. CBP does not have a national system for reporting and analyzing inspection statistics, and the data are generally not readily available by risk level (e.g., low, medium, high), were not uniformly reported, were difficult to interpret, and were incomplete. Further, we testified in March 2004, space limitations and safety concerns about inspection equipment constrain some ports in their utilization of screening equipment, which has affected the efficiency of examinations.[25] The Gilmore Commission made recommendations related to this challenge.

Directly related to the challenge of improving cargo container security are the challenges associated with the CBP's implementation of its Container Security Initiative, which allows CBP officials to screen for high-risk containers at key overseas ports, and its Customs-Trade Partnership against Terrorism (C-TPAT), which is designed to improve global supply chain security in the private sector. Both of these programs were launched quickly in an effort to secure ocean containers bound for the United States. However, a number of challenges must be overcome if these programs are going to accomplish the desired outcome and achieve long-term effectiveness. One of the these challenges is the development of human capital plans that clearly describe how CSI and C-TPAT will recruit, train, and retain staff to meet their growing demands as they expand to other countries and implement new program elements. Another challenge involves the expansion of efforts already initiated to develop performance measures for CSI and C-TPAT that include outcome-oriented indicators. Finally, strategic plans must be developed that clearly lay out CSI and C-TPAT goals, objectives, and detailed implementation strategies.

## Recapitalizing the U.S. Coast Guard

The continued recapitalization of the U.S. Coast Guard is specifically called for in the homeland security strategy. In 2002, the Coast Guard began its largest and most complex recapitalization challenge in its history, the Integrated Deepwater System program. As part of the Deepwater program, the Coast Guard is estimated to spend about $17 billion over 20 years to replace or modernize its fleet of cutters, aircraft, and communications equipment used for missions generally beyond 50

[25]See GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington, D.C.: Mar. 31, 2004)

miles from shore. Just 3 years into the program, the Coast Guard has already experienced management challenges. In March 2004,[26] we reported that key components needed for the Coast Guard to manage the program and oversee the system integrator's performance have not been effectively implemented. For example, we reported that the Coast Guard's integrated product teams have struggled to effectively collaborate and accomplish their missions, and management has not measured the extent of competition among suppliers or held the system integrator accountable for taking steps to increase competition in order to control future costs. In addition, in June 2004,[27] we expressed concern that the Coast Guard had not updated Deepwater's original 2002 acquisition schedule. We noted that maintaining a current acquisition schedule for programs of similar scope—such as those of the Department of Defense—is a fundamental and necessary practice. The Coast Guard's lack of an updated acquisition schedule makes it difficult to determine the degree to which the program is on track with its original schedule, lessens the Coast Guard's ability to monitor the contractor's performance, and may prevent the Department of Homeland Security and Congress from basing budget decisions on accurate information. As the Deepwater program matures, paying increased attention to address these outstanding program management and contractor oversight concerns will help the Coast Guard better meet current and future management challenges. The Gilmore Commission made recommendations related to this challenge.

[26]See GAO, *Contract Management: Coast Guard's Deepwater Program Needs Increased Attention to Management and Contract Oversight*, GAO-04-380 (Washington, D.C.: Mar. 9, 2004).

[27]See GAO, *Coast Guard: Deepwater Program Acquisition Schedule Update Needed*, GAO-04-695, (Washington, D.C.: June 9, 2004)

# Appendix IV: Domestic Counterterrorism

This appendix sets forth the definition and major initiatives of the Domestic Counterterrorism mission area and discusses the federal funding allocated, the agencies with major roles and the alignment of their strategic plans and implementation activities with the major initiatives, and a summary of the challenges faced by the nation. This appendix presents baseline information that can be used by Congress to provide oversight and track accountability for the initiatives in the Domestic Counterterrorism mission area.

## Definition and Major Initiatives

The National Strategy for Homeland Security categorizes homeland security activities into six mission areas, the third of which is Domestic Counterterrorism. This mission area includes the efforts of the nation's law enforcement agencies in identifying, halting, preventing, and prosecuting terrorists in the United States. Included in this mission area is the pursuit of individuals directly involved in terrorist activity, as well as their sources of support—the people and organizations that knowingly fund or provide material support or resources to the terrorists. It should be noted that this mission area is closely related to the Intelligence and Warning mission area in that activities that develop the basis for law enforcement action occur in that mission area and are carried out in this one.[1] Figure 7 shows an example of the type of activities carried out in the Domestic Counterterrorism mission area.

The strategy identifies the following major initiatives in the domestic counterterrorism mission area:

- improving intergovernmental law enforcement coordination,
- facilitating apprehension of potential terrorists,
- continuing ongoing investigations and prosecutions,
- completing FBI restructuring to emphasize prevention of terrorist attacks,
- targeting and attacking terrorist financing, and
- tracking foreign terrorists and bring them to justice.

[1]This definition is based on that used by OMB in its *2003 Report to Congress on Combating Terrorism* (Washington, D.C.: Sept. 2003).

**Figure 7: An FBI Evidence Response Team in Action at the Scene of a Terrorism-Related Exercise**

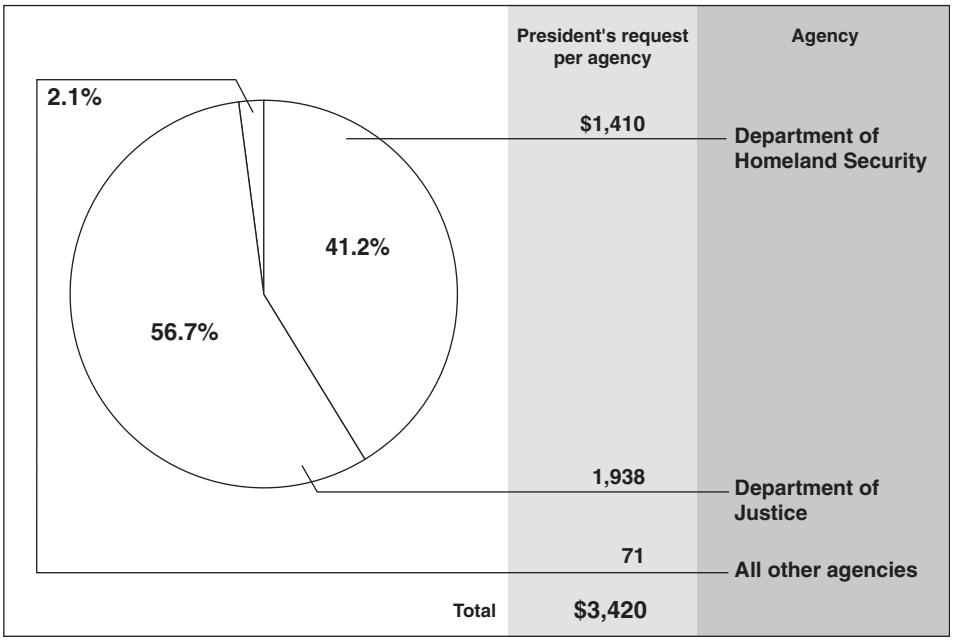
Source: GAO.

## Agencies with Major Roles in Domestic Counterterrorism

Of the six departments under review, DOJ and DHS have major roles in Domestic Counterterrorism. Within DOJ, the FBI works to detect and prevent terrorist acts through analysis and fieldwork to identify terrorists, their supporters, and materials that may be used to perpetrate a terrorist act, to include terrorist financing; tracks foreign terrorists and keeps them from entering the United States; and leads the multi-agency Joint Terrorism Task Forces (JTTF). In addition, DOJ's 94 United States Attorneys lead the Anti-Terrorism Advisory Councils, which enhance cooperation and information sharing among federal, state, and local law enforcement; first responders; industry; academia; and others. Within DHS, ICE, working with other law enforcement agencies, enforces laws related to the illegal presence of people and goods within the United States; detains those suspected of immigration-related violations and removes those convicted of immigration-related violations; and pursues criminal aliens, cases of identity theft or benefit fraud, human trafficking, money laundering, and other violations of such laws.

OMB reported that the total fiscal year 2005 funding request for the domestic counterterrorism mission area is just over $3.4 billion. DOJ accounts for $1.9 billion (57 percent) of these funds, primarily for the FBI. DHS accounts for another $1.4 billion (41 percent) of the funding request, mostly for ICE.[2] Figure 8 summarizes the fiscal year 2005 budget request for the domestic counterterrorism mission area by agency.

**Figure 8: Proposed Fiscal Year 2005 Homeland Security Funding for Domestic Counterterrorism**




Source: GAO, based on OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005.*

Notes: Budget authority in millions of dollars.

"All other agencies" includes the Departments of Transportation ($21 million) and Treasury ($46 million), as well as the Social Security Administration ($4 million).

OMB's reported data do not include funding for four departments that have activities under way in this mission area. These departments—Defense, Energy, Health and Human Services, and State—have either planning or implementation activity on specific initiatives, as discussed in

[2]OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005* (Washington, D.C.: Feb. 2004).

the next section of this appendix. On the basis of our previous work, we have noted several qualifications to OMB's figures to explain this discrepancy.[3] According to OMB officials, there is not always a clear distinction between homeland security activities and other related activities. The OMB staff must make judgment calls about how to characterize funding by mission areas. For example, some homeland security activities have multiple purposes ,and funding for these activities is allocated to different accounts that can cover multiple mission areas. In addition, some of the departments' activities, such as planning, coordination, or providing advice, may support Domestic Counterterrorism activities but are not included in the amounts shown.

## Alignment of Department Activities with the Major Initiatives

This section provides more detailed information about the Domestic Counterterrorism critical mission area initiatives, and the departments involved in conducting activities related to these initiatives. This includes a discussion of specific departmental planning and implementation activities, lead agency designations, and implementation activities in fiscal year 2004, with respect to each initiative. The data are summarized in table 9.

[3]See GAO, *Combating Terrorism: Funding Data Reported to Congress Should Be Improved*, GAO-03-170 (Washington, D.C.: Nov. 26, 2002).

**Table 9: Detailed Department Leadership and Planning/Implementation Activities in the Domestic Counterterrorism Mission Area's Six Initiatives**

| | DHS | | | DOJ | | | DOD | | | HHS | | | State | | | DOE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 |
| **Domestic counterterrorism** | | | | | | | | | | | | | | | | | | |
| (1) Improve intergovernmental law enforcement coordination | | ● | ● | ● | ● | ● | ● | ● | ● | | ● | ● | | | | ● | | ● |
| (2) Facilitate apprehension of potential terrorists | ● | ● | ● | ● | ● | ● | | | ● | | | | ● | ● | ● | | | |
| (3) Continue ongoing investigations and prosecutions | ● | ● | ● | ● | ● | ● | | | | | | | | | | | | |
| (4) Complete FBI restructuring to emphasize prevention of terrorist attacks | | | | ● | ● | ● | | | | | | | | | | | | |
| (5) Target and attack terrorist financing | | ● | ● | ● | ● | ● | | | | | | | ● | ● | ● | | | |
| (6) Track foreign terrorists and bring them to justice | ● | ● | ● | ● | ● | ● | ● | ● | ● | | | | ● | ● | ● | ● | | ● |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

PI = Prior implementation to fiscal year 2004
RP = Recent planning
04 = Fiscal year 2004 implementation

Source: GAO.

## Summary of Departmental Activities on the Initiatives

All six Domestic Counterterrorism initiatives are being addressed in the key departments' planning and implementation activities. As shown in table 9, at least one department cited activity in each of the six initiatives. At least four departments cited activity in three of the six initiative areas. For example, DHS, DOJ, DOD, and State implemented activities in the initiative, facilitating the apprehension of potential terrorists, during fiscal year 2004. DHS's ICE operated the Student and Exchange Visitor Information System computer network to identify and track nonimmigrants, foreign students, and exchange visitors while in the United States; DOJ's FBI continued to make improvements in the Integrated Automated Fingerprint Identification System; DOD expanded maritime interception and intelligence operations; and State bolstered the security of nations at high risk of terrorist transit by developing and installing Terrorist Interdiction Program software at their borders and training immigration officials in its use. Additionally, DHS, DOJ, and State demonstrated implementation activities in fiscal year 2004 related to targeting and attacking terrorist financing. DHS implemented Cornerstone, a comprehensive economic security program, targeting alternative

financing mechanisms that terrorists use to earn, move, and store funds. DOJ brought to bear several units and task forces to address terrorist financing and conducted criminal and intelligence investigations and prosecutions with respect to charities and banking; State cited diplomatic efforts to encourage countries to ratify and implement United Nations Security Council Resolution 1373, targeting terrorists' financing.

All six departments have been engaged in Domestic Counterterrorism initiatives. In contrast with DHS and DOJ, HHS only addressed a single initiative in this mission area (i.e., improving intergovernmental law enforcement coordination.) This limited initiative participation is understandable, given that the Domestic Counterterrorism mission area is primarily directed toward law enforcement. This is not a primary mission for HHS.

While we have identified department activities related to these initiatives, we did not determine the quality, status, or progress of such activities with respect to stated goals or targets within this mission area.

## Identification of Lead Agencies on the Initiatives

For all six initiatives, a lead agency is identified either in the strategy or the Homeland Security Presidential Directives. As shown in table 9, DOJ is a lead on the most initiatives—all six mission area initiatives. It is understandable for DOJ to have lead roles in each of these six initiatives given that the Domestic Counterterrorism critical mission area is primarily directed toward law enforcement-related initiatives (e.g., improving intergovernmental law enforcement coordination, facilitating the apprehension of potential terrorists, continuing ongoing investigations and prosecutions, and tracking foreign terrorists and bringing them to justice).

Additionally, DHS is a lead on three of the six initiatives (i.e., facilitating the apprehension of potential terrorists, continuing ongoing investigations and prosecutions, and tracking foreign terrorists and bringing them to justice); and State is a lead on one of six initiatives (facilitating the apprehension of potential terrorists). Three of the departments under review have not been identified as a lead on any Domestic Counterterrorism initiatives (DOD, HHS, and DOE) by the strategy and HSPDs since their missions are not primarily directed toward law enforcement.

The strategy and HSPDs identified multiple leads on three initiatives (see table 9). DHS, DOJ, and State are all leads on the initiative, facilitating the apprehension of potential terrorists; DHS and DOJ are both leads on the

remaining two initiatives (continuing ongoing investigations and prosecutions and tracking foreign terrorists and bringing them to justice). In addition, department strategic planning/implementation documents demonstrated that all identified leads in this mission area are clear leads.

## Fiscal Year 2004 Implementation of the Initiatives

In fiscal year 2004 implementation activity occurred with respect to each of the six initiatives (see table 9). DOJ implemented activity in 2004 on all 6 initiatives for which it was the lead; it also engaged in prior implementation in each of these six initiatives. DHS implemented prior and 2004 activity in each of the three initiatives for which it was identified as a lead (see illustrations above); and State cited both prior and fiscal year 2004 activity in the single initiative for which it was identified as a lead.

Additionally, several of the departments under review implemented multiple Domestic Counterterrorism initiatives for which they were not identified as a lead agency either in the strategy or in HSPDS. During fiscal year 2004, DOE cited implementation activities in two Counterterrorism initiatives, for which it was not identified as a lead (prior to fiscal year 2004, it conducted implementation activities in these same two initiatives.) DOD cited 2004 implementation activities in two of the six initiatives, without lead identification; and DHS and State both cited fiscal year 2004 implementation activities in two initiatives for which they were not identified as leads.

# Challenges in Domestic Counterterrorism

The attacks of September 11, and the catastrophic loss of life and property that resulted have redefined the mission of federal, state, and local law enforcement authorities. Accordingly, while organizations like the FBI continue to investigate and prosecute criminal activity, they are now assigning highest priority to preventing and interdicting terror activity within the United States. Our recent work in the Domestic Counterterrorism mission area has identified a number of challenges. These challenges include the need to transform the workforce and business practices of the FBI in order to focus on counterterrorism and intelligence-related priorities; attaining the level of interagency coordination necessary to leverage existing law enforcement resources for investigating money laundering and terrorist financing; developing databases for the collection and dissemination of alien information; and ensuring that law enforcement and other officials have the necessary training and expertise to detect counterfeit identification documents and identity fraud.

## Transforming the FBI to Focus on Counterterrorism

The strategy sets forth the nation's highest law enforcement objective as the prevention of terrorist attacks—a significant shift from pre-9/11 objectives. In order to focus the mission of the federal law enforcement community on prevention, in March 2004, we reported[4] that it is necessary for the federal government to restructure the FBI and other federal law enforcement agencies, reallocating certain resources and energies to the new prevention efforts. While the FBI has made significant progress in its transformation, it continues to face challenges in transforming its workforce and business practices to focus on counterterrorism and intelligence-related priorities. Additional challenges continue in the areas of human capital management and information technology, as well as in the intelligence and language services areas. The 9/11 Commission made recommendations related to this challenge.

## Effectively Investigating Terrorist Financing

The strategy provides that a "cornerstone" of the nation's domestic "counterterrorism effort involves a concerted interagency effort to target and interdict the financing of terrorist organizations and operations." Although terrorist financing is generally characterized by different motives than money laundering—a process by which the monetary proceeds from criminal activities are transformed into funds and assets that appear to have come from legitimate sources—the techniques used to obscure the origin of funds and their ultimate use are often quite similar. Therefore, Treasury, law enforcement agencies, other federal investigators, prosecutors, and financial regulators often employ similar measures and techniques in trying to detect and prevent both money laundering and terrorist financing.

In September 2003,[5] we reported that the annual National Money Laundering Strategy (NMLS)—which was required by 1998 federal

[4]See GAO, *FBI Transformation: FBI Continues to Make Progress in Its Efforts to Transform and Address Priorities*, GAO-04-578T (Washington, D.C.: Mar. 23, 2004); *FBI Reorganization: Progress Made in Efforts to Transform, but Major Challenges Continue*, GAO-03-759T (Washington, D.C.: June 18, 2003); *Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*, GAO-03-959 (Washington, D.C.: Sept. 25, 2003); *FBI Reorganization: Initial Steps Encouraging but Broad Transformation Needed*, GAO-02-865T (Washington, D.C.: June 21, 2002); *Foreign Languages: Workforce Planning Could Help Address Staffing and Proficiency Shortfalls*, GAO-02-514T (Washington, D.C.: Mar. 12, 2002); and *Foreign Languages: Human Capital Approach Needed to Correct Staffing and Proficiency Shortfalls*, GAO-02-375 (Washington, D.C.: Jan. 31, 2002).

[5]See GAO, *Combating Money Laundering: Opportunities Exist to Improve the National Strategy*, GAO-03-813 (Washington, D.C.: Sept. 26, 2003).

legislation—has had mixed results in guiding the efforts of law enforcement in the fight against money laundering and, more recently, terrorist financing. For example, although expected to have a central role in coordinating law enforcement efforts, interagency task forces created specifically to address money laundering and related financial crimes generally had not yet been structured and operating as intended and had not reached their expectations for leveraging investigative resources or creating investigative synergies. Also, most of the NMLS initiatives designed to enhance interagency coordination of money laundering investigations had not yet achieved their expectations. While the annual NMLS has fallen short of expectations, federal law enforcement agencies recognize the challenge of developing and using interagency coordination mechanisms to leverage existing resources to investigate money laundering and terrorist financing.

Additionally, regarding investigative efforts against sources of terrorist financing, our February 2004[6] report noted that a memorandum of agreement signed in May 2003 by the Attorney General and the Secretary of Homeland Security represents a partnering commitment by two of the nation's law enforcement agencies—the FBI and ICE, a component of DHS. Since the agreement was signed, progress has been made in waging a coordinated campaign against sources of terrorist financing. Continued progress will depend largely on the ability of the agencies to overcome the challenges associated with establishing and maintaining effective interagency relationships and meeting various other operational and organizational challenges, such as ensuring that the financial crimes expertise and other investigative competencies of both agencies are appropriately and effectively utilized.

The Bremer, Hart-Rudman, and 9/11 Commissions made recommendations related to the challenges presented in this section.

## Monitoring Alternative Financing Mechanisms

In addition to the challenge presented by interagency coordination issues, challenges exist in the monitoring of terrorists' use of alternative financing mechanisms. As we recommended in November 2003, the FBI, which leads terrorist financing investigations and maintains case data, should systematically collect and analyze data on terrorists' use of alternative

[6]See GAO, *Investigations of Terrorist Financing, Money Laundering, and Other Financial Crimes*, GAO-04-464R (Washington, D.C.: Feb. 20, 2004).

financing mechanisms.[7] Alternative financing mechanisms are outside the mainstream financial system and include the use of commodities (cigarettes, counterfeit goods, illicit drugs, etc.), bulk cash, charities, and informal banking systems to earn, move, and store assets. Cutting off terrorists' funding is an important means of disrupting their operations. As initial U.S. and foreign government deterrence efforts focused on terrorists' use of the formal banking or mainstream financial systems, terrorists may have been forced to increase their use of various alternative financing mechanisms. When agencies inform the FBI that an investigation has a terrorist component, the FBI opens a terrorism case. However, the FBI's data analysis programs do not designate the source of funding (i.e., specific charity, commodity, etc.) Without such data, the FBI will be challenged to conduct systematic analysis of trends and patterns focusing on alternative financing mechanisms from its case data. Without such an assessment, the FBI does not have analyses that could aid in assessing risk and prioritizing efforts. In response to our recommendation, the FBI conducted a onetime survey of its field offices to gather information about terrorist financing investigations since October 2001. Additionally, the FBI has instructed its field offices to update some of this information when new terrorist financing investigations are initiated. FBI officials told us that information from the surveys was entered into a database, and they believe that this database enables them to track information on alternative methods of terrorist financing and identify emerging trends, patterns, and funding sources. However, we have not evaluated the quality of the information provided. In addition, the FBI has not indicated how it has used this capability to perform an analysis of terrorist financing investigations. The Bremer, Hart-Rudman, and 9/11 Commissions also made recommendations related to this challenge.

## Detecting Identity Fraud

The strategy has an initiative to "coordinate suggested minimum standards for state driver's licenses." In September and October 2003,[8] we testified about the challenges to homeland security posed by identity fraud and how counterfeit identification can be easily produced and used to create fraudulent identities. Specifically, we conducted tests over the past several

[7]See GAO, *Terrorist Financing: U.S. Agencies Should Systematically Assess Terrorists' Use of Alternative Financing Mechanisms*, GAO-04-163 (Washington, D.C.: Nov. 14, 2003).

[8]See GAO, *Counterfeit Identification Raises Homeland Security Concerns*, GAO-04-133T (Washington, D.C.: Oct. 1, 2003); *Security Breaches at Federal Buildings in Atlanta, Georgia*, GAO-02-668T (Washington, D.C.: Apr. 30, 2002).

years that demonstrate how counterfeit identification documents can be used to obtain genuine state driver's licenses. In conducting these tests, we created fictitious identities and counterfeit identification documents using off-the-shelf computer graphic software that is available to any purchaser. These documents were then used to fraudulently obtain genuine driver's licenses in other states. Our work identified three basic challenges: (1) government officials and others generally did not recognize that the documents we presented were counterfeit; (2) many government officials were not alert to the possibility of identity fraud, and some failed to follow security procedures; and (3) identity verification procedures are inadequate. The weaknesses we found during this investigation clearly show that border inspectors need to have the means to verify the identity and authenticity of the documents that are presented to them. In addition, government officials who review identification need additional training in recognizing counterfeit documents. Further, these officials also need to be more vigilant when reviewing identification documents to the possibility of identification fraud. As we reported in October 2003,[9] directly related to the issue of detecting counterfeit documents and fictitious identities, is the importance of having sound practices for avoiding the improper issuance of Social Security numbers (SSNs) and ensuring the identity of those who receive them. Although originally created as a means of tracking worker earnings, the SSN has become a national identifier that is central to a range of transactions and services associated with American life, including obtaining a driver's license, opening a bank account, and establishing credit. Accordingly, SSNs are key pieces of information in creating false identities. In prior work we recommended that the Social Security Administration verify the documents of all SSN applicants and reassess its policies for issuing replacement cards, which allowed an individual to obtain up to 52 per year. The recently passed Intelligence Reform and Terrorism Prevention Act of 2004 has specific provisions to address our recommendations. Additionally, the 9/11 Commission made recommendations related to this challenge.

[9]See GAO, *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.: Oct. 15, 2003).

# Appendix V: Protecting Critical Infrastructures and Key Assets

This appendix sets forth the definition and major initiatives of the Protecting Critical Infrastructures and Key Assets mission area and discusses the agencies with major roles, their funding, the alignment of their strategic plans and implementation activities with the major initiatives, and a summary of the challenges faced by the nation. This appendix provides baseline information that can be used by Congress to provide oversight and track accountability for the initiatives in the Protecting Critical Infrastructures and Key Assets mission area.

## Definition and Major Initiatives

The *National Strategy for Homeland Security* categorizes homeland security activities into six mission areas, the fourth of which is protecting critical infrastructures and key assets. This mission area—commonly referred to as Critical Infrastructure Protection (CIP)—includes programs that improve protection of the interconnecting sectors that make up the nation's critical infrastructure. The sectors are agriculture, banking and finance, chemical and hazardous materials, emergency services, defense industrial base, energy, food, government, information technology and telecommunications, postal and shipping, public health and health care, transportation, and drinking water and water treatment systems. Programs associated with the physical or cyber security of federal assets also belong in this mission area. Finally, programs designed to protect the nation's key assets—unique facilities, sites, and structures whose disruption or destruction could have significant consequences—are also included in this mission area.[1] In addition to the homeland security strategy, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* and the *National Strategy to Secure Cyberspace* provide detailed discussions of Critical Infrastructure Protection. Figure 9 shows an example of the type of activities carried out in the Critical Infrastructure Protection mission area.

The homeland security strategy identifies the following major initiatives in the critical infrastructure protection mission area:

- unifying America's infrastructure protection effort in the Department of Homeland Security,
- building and maintaining a complete and accurate assessment of America's critical infrastructure and key assets,

[1]This definition is from OMB's *2003 Report to Congress on Combating Terrorism* (Washington, D.C.: Sept. 2003).

- enabling effective partnership with state and local governments and the private sector,
- developing a national infrastructure protection plan,
- securing cyberspace,
- harnessing the best analytic and modeling tools to develop effective protective solutions,
- guarding America's critical infrastructure and key assets against "inside" threats, and
- partnering with the international community to protect our transnational infrastructure.

**Figure 9: A U.S. Immigration and Customs Enforcement Helicopter Patrols the Skies over the Nation's Capital**

Source: U.S. Immigration and Customs Enforcement.

## Agencies with Major Roles in Critical Infrastructure Protection

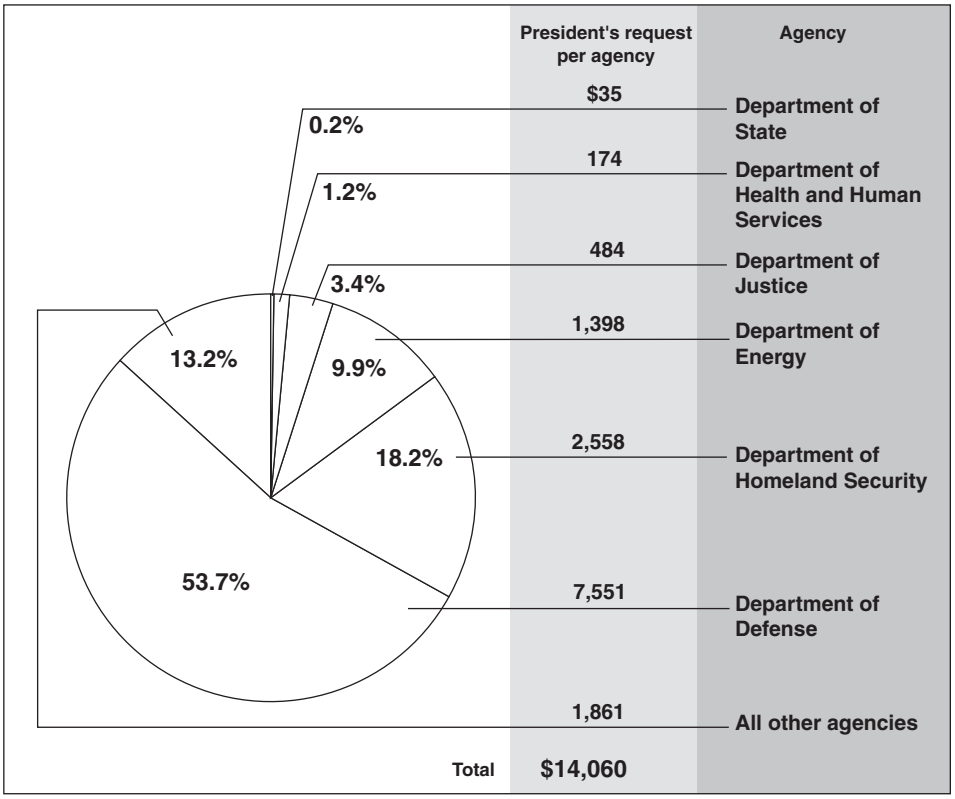
Of the six departments under review, DHS, DOD, DOE, and DOJ have major roles in Critical Infrastructure Protection. DHS has primary responsibility for emergency services, government, information and telecommunications, transportation, chemicals, and postal and shipping sectors. Examples of specific functions performed by DHS include the protection of federally owned or leased properties throughout the country by the Federal Protective Service, the Secret Service's role in coordinating

site security plans at designated special security events, and the National Cyber Response Coordination Group's role as a coordinating body for cyber emergencies of national scope. DOD is active in this mission area, primarily in areas of physical security of military and military-related activities, installations, and personnel. DOE'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. DOJ, primarily through work done by the FBI 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.

OMB reported that the total fiscal year 2005 funding request for the critical infrastructure protection mission area is $14 billion. DOD has the largest share of this funding ($7.6 billion, or 54 percent) for programs focusing on physical security and improving the military's ability to prevent or mitigate the consequences of attacks against its personnel and installations. DHS accounts for $2.6 billion (18 percent) of 2005 funding. A total of 26 other agencies report funding to protect their own assets and to work with states, localities, and the private sector to reduce vulnerabilities in their areas of expertise.[2] Figure 10 summarizes the fiscal year 2005 budget request for the CIP mission area by agency.

[2]OMB, *Analytical Perspectives*, *Budget of the United States Government*, *Fiscal Year 2005* (Washington, D.C.: Feb. 2004).

**Figure 10: Proposed Fiscal Year 2005 Homeland Security Funding for Critical Infrastructure Protection**




Source: GAO, based on OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005.*

Notes: Budget authority in millions of dollars.

"All other agencies" includes USDA ($166 million) and the Department of Transportation ($189 million), as well as the National Aeronautics and Space Administration ($207 million), the National Science Foundation ($317 million), the Social Security Administration ($151 million), and several others ($866 million). Total does not add up to 100 because of rounding.

## Alignment of Department Activities with the Major Initiatives

This section provides more detailed information about the CIP mission area initiatives and the departments involved in conducting activities related to these initiatives. This includes a discussion of specific departmental planning and implementation activities, lead agency designations, and implementation activities in fiscal year 2004, with respect to each initiative. The data are summarized in table 10.

**Table 10: Detailed Department Planning/Implementation Activities in the Protecting Critical Infrastructures and Key Assets Critical Mission Area's Eight Initiatives**

| | DHS | | | DOJ | | | DOD | | | HHS | | | State | | | DOE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 |
| **Protecting critical infrastructures and key assets** | | | | | | | | | | | | | | | | | | |
| (1) Unify America's infrastructure protection effort in DHS | | ● | ● | ● | | | ● | ● | ● | | ● | ● | | | | ● | | ● |
| (2) Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets | ● | ● | ● | ● | | | | ● | ● | ● | ● | ● | | | | ● | | ● |
| (3) Enable effective partnership with state and local governments and the private sector | | ● | ● | ● | ● | ● | | ● | | | ● | ● | | | | ● | | ● |
| (4) Develop a national infrastructure protection plan | | ● | ● | | | | | ● | | | ● | | | | | ● | ● | ● |
| (5) Secure cyberspace | | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | | ● | ● |
| (6) Harness the best analytic and modeling tools to develop effective protective solutions | | ● | ● | | | | | ● | ● | | ● | ● | | | | ● | | ● |
| (7) Guard America's critical infrastructure and key assets against "inside" threats | ● | ● | ● | | | | ● | ● | | | ● | ● | ● | ● | ● | ● | ● | ● |
| (8) Partner with the international community to protect our transnational infrastructure | | ● | ● | ● | ● | ● | ● | ● | ● | | ● | ● | ● | ● | ● | | | |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Department IMPLICITLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

PI = Prior implementation to fiscal year 2004
RP = Recent planning
04 = Fiscal year 2004 implementation

Source: GAO.

## Summary of Departmental Activities on the Initiatives

All eight CIP initiatives are being addressed by key departments' planning and implementation activities. At least three departments (DHS, DOD, and HHS) cited activity in each of the eight initiatives (see table 10). For example, DHS, HHS, State, and DOE each implemented activities in fiscal year 2004 with respect to guarding America's critical infrastructure and key assets against inside threats. DHS started the Transportation Worker Identification Credential program to enhance access security across the nation's transportation system; the Food and Drug Administration within HHS, issued guidance to the food industry that suggested preventive measures, including employee background checks, which could increase the security of food while under an establishment's control; State developed diplomatic agreements with Mexico and Canada to permit background checks of truck drivers; and DOE conducted selected polygraph examinations and financial disclosures of those working in the

energy field. Additionally, DHS, DOJ, DOD, HHS, State, and DOE each demonstrated implementation activities in fiscal year 2004 with respect to securing cyberspace. For example, DHS's Information Analysis and Infrastructure Protection Directorate refined, updated, and monitored the implementation of a national plan to protect physical and cyber critical infrastructures; DOJ operated a Special Technologies and Applications Section within the Cyber Division to support counterterrorism, counterintelligence, and criminal investigations involving computer intrusions; DOD prepared a departmentwide plan for CIP and physical and cyber assets; HHS's Centers for Disease Control and Prevention issued a fiscal year 2004 cyber security plan that includes activities and metrics; State took steps to strengthen the network's intrusion and detection capabilities; and DOE drafted a comprehensive Critical Infrastructure Plan, including plans for securing cyberspace.

All six departments have been engaged in CIP initiatives. While we have identified department activities related to these initiatives, we did not determine the quality, status, or progress of such activities with respect to stated goals or targets within this critical mission area.

## Identification of Lead Agencies on the Initiatives

For all eight initiatives, a lead agency was identified either in the homeland security strategy or HSPDs. As shown in table 10, DHS is a lead on all eight initiatives. It seems appropriate that DHS would be the department with the most initiative leads, given that the "national vision" put forth in the strategy calls for DHS "to work with the federal departments and agencies, state and local governments, and the private sector to implement a comprehensive national plan to protect critical infrastructure and key assets." It also seems appropriate that State would have a lead on matters of international critical infrastructure protection, given its overseas mission (partnering with the international community to protect our transnational infrastructure). The four remaining departments each have a lead on one mission area initiative. DOD, HHS, and DOE are all leads on the same initiative—building and maintaining a complete and accurate assessment of America's critical infrastructure and key assets. These departments have the sector leads as follows: DOD for defense industrial base, HHS for public health, and DOE for the energy sector. DOJ has a leading role in securing cyberspace, owing to its investigative and prosecutorial role in reducing threats in cyberspace.

In all, the homeland security strategy and HSPDs identified multiple leads on three of the eight mission area initiatives. The five initiative exceptions that do not have multiple leads are unifying America's infrastructure

protection effort in DHS, enabling effective partnership with state and local governments and the private sector, developing a national infrastructure protection plan, harnessing the best analytic and modeling tools to develop effective protective solutions, and guarding America's critical infrastructure and key assets against inside threats. DOD, HHS, and DOE are identified as clear leads on a single initiative; DHS is identified as a clear lead on six of its eight initiative leads; and DOJ and State are implied leads on the single initiatives they lead.

DOJ had been identified as a lead agency with respect to enabling effective partnerships with state and local governments and the private sector. However, given the transfer of the National Infrastructure Protection Center programs to the Department of Homeland Security, DOJ officials indicated that the department no longer serves as a lead on that initiative.

## Fiscal Year 2004 Implementation of the Initiatives

In fiscal year 2004, implementation activity occurred with respect to all eight initiatives (see table 10). DHS implemented activity in all eight initiatives for which it was identified as a lead; DOJ, DOD, HHS, State, and DOE implemented activity in fiscal year 2004 in each of the initiatives for which they had been identified as a lead.

Additionally, several of the departments under review implemented multiple CIP initiatives for which they were not identified as a lead in the strategy and HSPD. During fiscal year 2004, HHS cited implementation activity on six mission area initiatives for which it is was not given a lead role (it cited prior implementation on one of these initiatives); DOE cited 2004 implementation activity on six initiatives for which it is not the lead (with prior implementation on five); DOJ cited 2004 implementation activity on two initiatives for which it was not a lead (with prior implementation on four); and State cited 2004 and prior implementation on two initiatives, for which it was not identified as a lead.

Our analysis further indicates that three departments transferred programs, systems, or centers to the newly formed DHS, within this critical mission area. DOJ transferred the Key Asset Identification program, a component of the National Infrastructure Protection Center, to DHS. In accordance with the Homeland Security Act of 2002, DOD transferred the National Communication System. DOE transferred the National Infrastructure Simulation and Analysis Center and some related programs oriented toward protecting key infrastructure facilities and their components.

## Challenges in Critical Infrastructure Protection

As the *National Strategy for Homeland Security* points out, "protecting America's critical infrastructures and key assets is a formidable challenge" because "our open and technologically complex society presents an almost infinite array of potential targets, and our critical infrastructure changes as rapidly as the marketplace." In fact, the mission area is so diverse that two additional strategies—the *National Strategy for the Physical Protection of Critical Infrastructures and Key Asset*s and the *National Strategy to Secure Cyberspace*—were issued to supplement the homeland security strategy. Our recent work in the CIP mission area has identified a number of challenges. These challenges include those related to the federal government's role in managing CIP. Among these are developing a comprehensive and coordinated national CIP plan that delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interims objectives and milestones, sets time frames for achieving objectives, and establishes performance measures. In addition to identifying the challenges related to the overall management of CIP, our work has identified numerous challenges within specific infrastructure sectors. Included here are improving the security of government facilities; implementing better training and procedures to detect counterfeit documents and identity fraud; analyzing the strengths, interdependencies, and vulnerabilities of the financial services sector and developing strategies for responses to terrorist events; improving the safety and security of the postal system; strengthening security with regard to drinking water utilities; addressing the terrorist threat to agriculture and food; and addressing security issues with regard to chemical plants, nuclear power plants, and nuclear weapons sites.

## Effectively Managing Critical Infrastructure Protection

The homeland security strategy specifically calls for the development of a "national infrastructure protection plan." The challenges identified in this mission area include those related to the federal government's role in managing CIP. To ensure the coverage of the critical infrastructure sectors identified in the homeland security strategy, HSPD-7[3] designated a sector-specific agency for each sector. This agency is responsible for infrastructure protection activities within its assigned area and for coordinating and collaborating with other relevant agencies—as well as

[3]In December 2003, the President issued HSPD-7, which established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources and to protect them from terrorist attacks. It superseded Presidential Decision Directive 63 and defines responsibilities for DHS, sector-specific agencies (formerly referred to as sector liaisons) and other departments and agencies.

state and local governments, and the private sector—to carry out its mission. In addition, DHS's Information Analysis and Infrastructure Protection Directorate (IAIP) has the responsibility to (1) develop a comprehensive national CIP plan consistent with the Homeland Security Act of 2002; (2) recommend CIP measures in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities; and (3) disseminate, as appropriate, information analyzed by the department both within DHS and to other federal agencies and private sector entities. Regarding the national CIP plan, according to HSPD-7, it is to be produced by December 2004 and outline national goals, objectives, milestones, and key initiatives. IAIP is also tasked with coordinating with other federal agencies to administer the Homeland Security Advisory System to provide specific warning information along with advice on appropriate protective measures and countermeasures.

Over the last several years, we have reviewed various aspects of federal and private sector CIP efforts and issued numerous related reports. In an April 2004 testimony,[4] we made numerous recommendations related to the federal CIP efforts, including issues involving the functions and responsibilities transferred to DHS, that represent challenges to DHS and other federal agencies. Among these challenges are

- developing a comprehensive and coordinated national CIP plan that delineates roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets time frames for achieving objectives, and establishes performance measures;

- developing fully productive information-sharing relationships within the federal government and among the federal government and state and local governments and the private sector; and.

- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector.

[4]See GAO, *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors*, GAO-04-699T (Washington, D.C.: Apr. 21, 2004).

The Bremer, Gilmore, Hart-Rudman, and 9/11 Commissions all made recommendations related to the challenges presented in this section.

## Improving Security at Government Facilities

The homeland security strategy identifies government operations as a critical infrastructure sector. In addition, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, which provides guidance in implementing the *Homeland Security Strategy*, states that the General Services Administration (GSA) is the principal agency responsible for the management of federal government facilities. Additional departments and agencies are similarly involved in the management of federally owned or operated facilities, including DOD and the Department of Veterans Affairs (VA). Furthermore, a challenge identified in the strategy is that most government organizations occupy buildings that are also used by a variety of nongovernmental tenants, such as shops and restaurants where the public is able to move about freely. The strategy also states that private owners of these properties may not want or have the ability to modify their procedures to accommodate the increased or special security countermeasures required by their federal tenants, such as installing surveillance cameras in lobbies, redesigning entry points to restrict the flow of traffic, or setting up x-ray machines and metal detectors at these entrances. To overcome protection challenges associated with government facilities, DHS plans to

- develop a process to screen nonfederal tenants and visitors entering private sector facilities that house federal organizations,
- determine the criticality and vulnerability of government facilities,
- develop long-term construction standards for facilities requiring specialized security measures, and
- implement new technological security measures at federally occupied facilities.

In part because of the challenges associated with protecting government facilities, we designated federal real property as a high-risk area in January 2003.[5] As the government's security efforts intensify, the government will be faced with important questions regarding the level of security needed to adequately protect federal facilities and how the security community should proceed. Furthermore, real property managers will have to

[5]See GAO, *High-Risk Series: Federal Real Property*, GAO-03-122 (Washington, D.C.: Jan. 1, 2003).

dedicate significant staff time and other human capital resources to security issues and thus may have less time to manage other problems. Another broader effect is the impact that increased security will have on the public's access to government offices and other assets. Debate arose in the months after September 11, and continues to this day on the challenge of providing the proper balance between public access and security.

Finally, as we testified in April 2002 and again in September 2003,[6] an additional challenge to ensuring the proper security of federal buildings is the ease with which counterfeit identification or identity fraud can be used to breach security. Our work identified three basic challenges in this regard: (1) government officials and others generally did not recognize that the documents we presented were counterfeit; (2) many government officials were not alert to the possibility of identity fraud, and some failed to follow security procedures; and (3) identity verification procedures are inadequate. The weaknesses we found during these investigations clearly show those government officials who review identification need additional training in recognizing counterfeit documents. Further, these officials also need to be more vigilant when searching for identification fraud.

Both the Gilmore and 9/11 Commissions made recommendations related to the challenges discussed above.

## Addressing Issues Involving the Federal Protective Service

As the agency with primary responsibility for carrying out the protection of thousands of federal facilities, the Federal Protective Service (FPS), which transferred from the GSA to DHS in March 2003, plays a critical role in the federal government's defense against terrorism. However, in July 2004, we reported that FPS faces significant challenges in carrying out its responsibilities.[7] One challenge involves the agency's expanding mission and increased responsibility. FPS already has responsibility for securing approximately 8,800 GSA government-occupied facilities and plans to take on additional DHS facilities. It may also seek authority to protect other federal facilities. Additionally, the agency's mission has expanded to include other homeland security functions, such as supporting efforts to apprehend foreign nationals suspected of illegal activity. In light of these

[6]See GAO-02-668T and *Counterfeit Identification and Identification Fraud Raise Security Concerns*, GAO-03-1147T (Washington, D.C.: Sept. 9, 2003)

[7]See GAO, *Homeland Security: Transformation Strategy Needed to Address Challenges Facing the Federal Protective Service*, GAO-04-537 (Washington, D.C.: July 14, 2004).

changes, however, it does not have a transformation strategy to address its expanding mission as well as the other challenges it is facing. Among these other challenges are resolving issues related to the agency's funding and the transfer of its mission-support functions to DHS.

## Addressing Vulnerabilities of the Financial Services Sector

As stated in the homeland security strategy, the financial services sector is essential to sustaining the economy of the United States. Accordingly, the entities and networks that constitute the U.S. financial system are among the critical infrastructure that face increasing threats from terrorist and other disruptions. Transactions involving trillions of dollars occur in the U.S. financial markets annually. After the large-scale impact on market participants that resulted from the September 11 attacks, law enforcement and other government organizations reported that key institutions and communications networks that support the financial markets have been specifically identified as targets.

As we reported in February 2003, and September 2004, the government entities responsible for key financial market participants have begun to take actions to ensure that financial institutions are taking steps to minimize disruptions from terrorist attacks, but challenges remain.[8] For example, although banking and securities regulators have issued standards for the financial market participants that perform key roles in the clearance and settlement process through which the payments and ownership transfers resulting from securities trading are made, these regulators had not conducted a formal analysis of the readiness of financial market participants to better ensure that trading in critical U.S. financial markets could also resume smoothly and in a timely manner after a major disaster.[9] Among the challenges that these regulators face is that thousands of entities are active in the financial markets, and they must ensure that sufficient numbers take adequate steps to allow fair and orderly trading to resume. Ensuring sufficient actions are taken by the

[8]See GAO, *Financial Market Preparedness: Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters*, GAO-04-984 (Washington, D.C.: Sept. 27, 2004); *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, GAO-03-251 (Washington, D.C.: Feb. 12, 2003); and *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, GAO-03-414 (Washington, D.C.: Feb. 12, 2003).

[9]*Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.* Board of Governors of the Federal Reserve, Office of the Comptroller of the Currency, and the Securities Exchange Commission (Washington, D.C.: Apr. 8, 2003).

private sector organizations that participate in the financial markets is also a challenge for securities r, and thus the extent to which they implement business continuity plans that would allow them to resume activities is a business decision.

Another challenge facing the financial sector is implementing the strategy—developed by industry representatives under the sponsorship of the U.S. Department of the Treasury—that discusses additional efforts necessary to identify, assess, and respond to sectorwide threats. For example, the sector is expected to analyze its infrastructure's strengths, interdependencies, and vulnerabilities and develop strategies for responses to events. However, we reported in January 2003 that the financial services sector has not developed specific interim objectives;[10] detailed tasks, time frames, or responsibilities for implementation; or a process for monitoring progress. Without completing such steps, a greater risk exists that the financial sector's efforts will be less focused, efficient, and effective.

## Improving Postal and Shipping Security

Another critical infrastructure sector identified in the homeland security strategy is postal and shipping. In our May 2003 testimony,[11] we reported that one of the challenges faced in this sector is that it is particularly vulnerable to being used as a means of delivering terrorist attacks. For example, anthrax was sent through the mail in October 2001, resulting in the death of five people, including two postal workers in Washington, D.C., and potentially exposed hundreds more to this lethal substance. Moreover, use of the mail as a vehicle for transmitting anthrax or similar weapons threatens the nation's mail stream and places the American public at risk. To help address this challenge, DHS has a role in mail security as part of its overall homeland security mission, in support of the two agencies that

[10]See GAO, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, GAO-03-173 (Washington, D.C.: Jan. 30, 2003).

[11]GAO, *Diffuse Security Threats: USPS Air Filtration Systems Need More Testing and Cost Benefit Analysis before Implementation*, GAO-02-838 (Washington, D.C.: Aug. 22, 2002*); U.S. Postal Service: Better Guidance Is Needed to Improve Communication Should Anthrax Contamination Occur in the Future*, GAO-03-316 (Washington, D.C.: Apr. 7, 2003); U.*S. Postal Service: Issues Associated with Anthrax Testing at the Wallingford Facility*, GAO-03-787T (Washington, D.C.: May 19, 2003); *U.S. Postal Service: Clear Communication with Employees Needed before Reopening the Brentwood Facility.* GAO-04-205T (Washington, D.C.: Oct. 23, 2003); and *Federal Mail Screening: Better Postal Service Communication with Agencies Needed to Enhance Federal Mail Security in the Washington, D.C., Area*, GAO-04-286RNI (Washington, D.C.: Dec. 31, 2003).

have key roles—the United States Postal Service (USPS) and GSA. Under the Homeland Security Act of 2002, DHS is responsible for, among other things, protecting certain buildings, grounds, and property owned or secured by the federal government and identifying and assessing current and future threats to the homeland. In addition, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* states DHS has a role in determining the criticality and vulnerability of government facilities, including federal mail centers. Following the anthrax attacks, USPS established increased security procedures to protect mail destined for federal agencies in the Washington, D.C., area, including the irradiation of mail. At the same time, federal agencies have taken various steps to increase the security of their mail centers in order to protect federal workers and buildings from possible exposure to anthrax and other types of dangerous material, such as explosives. In our December 2003 review of mail security in the executive branch, we determined that a lack of information from USPS on mail security incidents, as well as on mail security policies and practices, reduced the ability of federal agencies to make well-informed decisions regarding mail practices or their future plans for mail screening. In addition, we found that agencies' fear of cross-contamination influenced their decision to implement practices which were not recommended by the USPS or other government and industry sources of mail-screening information. USPS and GSA have recognized that agencies need more information and have taken steps in the right direction. We recommended that USPS and GSA further work together as appropriate to establish mechanisms for providing federal agencies with USPS mail security policies and procedures, the risks associated with various classes of mail and the rationales behind these assessments, and USPS's future plans in federal mail security, and include DHS as appropriate in addressing these recommendations.

## Strengthening Drinking Water Security

The homeland security strategy also identifies water as a critical infrastructure sector. Damage or destruction of drinking water systems by terrorists could disrupt not only the availability of safe drinking water, but also the delivery of vital services that depend on these water supplies, such as fire suppression. In our October 2003 report,[12] we identified several key physical assets within this sector that are highly vulnerable to terrorist attacks. Specifically, the distribution system, source water

[12]See GAO, *Drinking Water: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security*, GAO-04-29 (Washington, D.C.: Oct. 31, 2003).

supplies, critical information systems, and chemicals stored on-site that are used in the treatment process have been identified as potential targets of terrorism. Additionally, our work has identified vulnerability challenges that may involve multiple system components or even an entire drinking water system. Chief among these challenges are (1) a lack of redundancy in vital systems, which increases the likelihood that an attack could render a system inoperable; and (2) the difficulty many systems face because of a lack of information on the most serious threats to which they are exposed.

Additional challenges relate to the criteria for determining how federal funds should be allocated among drinking water systems to improve their security, and the methods for distributing those funds, as well as specific activities the federal government should support to improve drinking water security. With regard to the allocation of federal funds, our work indicates that utilities serving high-density areas deserve at least a high priority for federal funding. Other utilities warranting priority are those serving critical assets, such as military bases, national icons, and key academic institutions. Regarding specific security-enhancing activities most deserving of federal support, we found that challenges that must be overcome include implementing physical and technological upgrades to improve security; researching and developing technologies to prevent, detect, or respond to an attack (particularly near-real-time monitoring technologies); providing education and training to support simulation exercises; conducting specialized training and multidisciplinary consulting teams; and strengthening key relationships between water utilities and other agencies that may have key roles in an emergency response.

## Addressing Agriculture and Food Supply Security

Another critical infrastructure sector identified in the homeland security strategy is the nation's food supply. While our food supply is generally safe and plentiful, each year tens of millions of Americans become ill and thousands die from eating unsafe food. The current federal food safety system is challenged by its fragmentation, which results in inefficient, inconsistent, and overlapping programs and operations. We have long recommended the establishment of a single food safety agency to administer a uniform, risk-based inspection system. Since the terrorist attacks of September 11, ensuring the security of our food—that is, protecting it from deliberate contamination—has become an added challenge for the federal agencies responsible for protecting the food and agriculture sectors of our economy.

As we have reported in numerous reports and testimonies over the last decade,[13] our fragmented federal food safety system hampers the efficiency and effectiveness of food safety efforts. Federal agencies have overlapping oversight responsibilities, which result in inefficient use of inspection resources and enforcement. This system is now further challenged by the realization that American farms and food are vulnerable to deliberate contamination. Fundamental changes are needed to improve the effectiveness and efficiency of the federal food safety system and to protect the nation's food supply from acts of deliberate contamination.

One challenge involves the fact that bioterrorism attacks could be directed at many different targets in the farm-to-table continuum, including crops, livestock, and food products in the processing and distribution chain. For example, experts believe that terrorists would attack livestock and crops if their primary intent were to cause severe economic dislocation. On the other hand, if their motives were to harm humans, they could decide to contaminate finished food products. While agencies have taken steps to better protect the food supply, for the most part, the nation must still rely on the current food safety system to respond to bioterrorism acts against it.[14] An additional challenge relates to the broad authority that agencies have to regulate the safety of the U.S. food supply but not the security of it. As a result, federal agencies are beginning to explore the extent to which food processors are voluntarily implementing security measures to protect against deliberate contamination.[15] Finally, a challenge involves protecting against animal diseases that could be accidentally—or deliberately—introduced into the country. Certain animal disease can be devastating to the agricultural economy while others, such as mad cow disease, can be transmitted to humans. Our recent work has raised serious questions about security at DHS's Plum Island Animal Disease Center, which is responsible for developing strategies to protect the nation against animal

[13]See GAO, *Federal Food Safety and Security System: Fundamental Restructuring is Needed to Address Fragmentation and Overlap*, GAO-04-588T (Washington, D.C.: Mar. 30, 2004).

[14]See GAO, *Bioterrorism: A Threat to Agriculture and the Food Supply*, GAO-04-259T (Washington, D.C.: Nov. 19, 2003).

[15]See GAO, *Food-Processing Security: Voluntary Efforts Are Under Way, but Federal Agencies Cannot Assess Their Implementation*, GAO-03-342 (Washington, D.C.: Feb. 14, 2003).

diseases.[16] In particular, we had concerns about the adequacy of the facility's controls of dangerous pathogens.[17]

The Gilmore Commission made recommendations related to the challenges presented in this section.

## Addressing Chemical Plant Security

Although the chemical industry is identified in the homeland security strategy as a critical infrastructure sector, we reported in March 2003 that the federal government has not comprehensively assessed the industry's vulnerability to terrorist attacks.[18] As a result, federal, state, and local entities are challenged by a lack of comprehensive information on the vulnerabilities faced by the sector. An additional challenge concerns the fact that no federal laws explicitly require all chemical facilities to take security actions to safeguard their facilities against a terrorist attack. Moreover, while federal laws require some facilities to take security precautions, federal requirements do not address security at all facilities that produce, use, or store hazardous chemicals.

Although the chemical industry has undertaken a number of voluntary initiatives to address security concerns at chemical facilities, the extent of participation in voluntary initiatives is unclear. The chemical industry faces significant challenges in preparing its facilities against terrorist attack, including ensuring that facilities obtain adequate threat information, determining the appropriate security measures given the level of risk, and ensuring that all facilities that house hazardous chemicals address security concerns.

[16] USDA's Plum Island Animal Disease Center was transferred to DHS in June of 2003. Although USDA still administers research and diagnostic programs on the island, DHS and USDA also conduct joint research supporting efforts to reduce the effects of an attack on agriculture. DHS is responsible for the security and management of the facility. Located off the northeast coast of Long Island, New York, the center is the only place in the United States where certain highly infectious foreign animal diseases, such as foot and mouth disease, are studied.

[17] See GAO, *Combating Bioterrorism: Actions Needed to Improve Security at Plum Island Animal Disease Center*, GAO-03-847 (Washington, D.C.: Sept. 19, 2003).

[18] See GAO, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown*, GAO-03-439 (Washington, D.C.: Mar. 14, 2003).

DHS and the Environmental Protection Agency (EPA) have taken steps to identify high-risk facilities, develop appropriate information-sharing mechanisms, and develop a legislative proposal to require chemical facilities to expeditiously assess their vulnerability to terrorist attacks and, where necessary, require these facilities to take corrective action. Legislation is now before Congress that, if enacted, would direct DHS, or DHS and EPA, to require chemical facilities to address these challenges.[19]

## Challenge: Addressing Nuclear Power Plant Security

Another critical infrastructure sector identified in the homeland security strategy is energy. Among the possible terrorist targets within this sector are the nation's nuclear power plants—104 facilities containing radioactive fuel and waste. The Nuclear Regulatory Commission (NRC) oversees security of these facilities through an inspection program designed to verify the plants' compliance with security requirements. However, in September 2003,[20] we reported that NRC faces challenges in ensuring that its oversight programs are effective in safeguarding these facilities and the surrounding communities. Specifically, three aspects of its security inspection program reduced NRC's effectiveness in this area. First, NRC's inspectors often used a process that minimized the significance of security problems found in annual inspections by classifying them as "non-cited violations" if the problem had not been identified frequently in the past or if the problem had no direct, immediate, or adverse consequences at the time it was identified. By making extensive use of these non-cited violations for serious problems, NRC may overstate the level of security at a power plant and reduce the likelihood that needed improvements are made. Second, NRC does not have a routine, centralized process for collecting, analyzing, and disseminating security inspections to identify problems that may be common to plants or to provide lessons learned in resolving security problems. Such a mechanism may help plants improve their security. Third, although NRC's force-on-force exercises can demonstrate how well a nuclear power plant might defend itself against a real-life threat, several weaknesses in how NRC conducts these exercises limited their usefulness. Weaknesses included using (1) more personnel to defend the plant during these exercises than would be available on a

[19]See GAO, *Homeland Security: Federal Action Needed to Address Security Challenges at Chemical Facilities*, GAO-04-482T (Washington, D.C.: Feb. 23, 2004).

[20]See GAO, *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened*, GAO-03-752 (Washington, D.C.: Sept. 4, 2003).

normal day, (2) attacking forces that are not trained in terrorist tactics, and (3) unrealistic weapons (rubber guns) that do not simulate actual gunfire. We also found that NRC made only limited use of some available improvements that would make force-on-force exercises more realistic and provide a more useful training experience. Finally, even if NRC strengthens its inspection program, commercial nuclear power plants face legal challenges in ensuring plant security. First, federal law generally prohibits guards at these plants from using automatic weapons, even though terrorists are likely to be using them. Second, state laws vary regarding the permissible use of deadly force and the authority to arrest and detain intruders, and we found that guards are unsure about the extent of their authorities and may hesitate or fail to act if the plant is attacked.

## Effectively Securing Nuclear Weapons Sites

The homeland security strategy identifies the defense industrial base as a critical infrastructure sector. Within this sector, DOE has responsibility for sites containing nuclear weapons or the materials used in making nuclear weapons. A terrorist attack on one of these sites could have devastating consequences for the site and its surrounding communities. In ensuring that these sites are adequately prepared to defend themselves against the higher terrorist threats present in a post-September 11, world, DOE faces significant challenges. Among the challenges identified in our April 2004 report[21] are the development of a new design basis threat (DBT), a classified document that identifies, among other things, the potential size and capabilities of terrorist forces. While the May 2003 DBT identified a larger terrorist threat than did the 1999 DBT,[22] further analysis by DOE, in response to GAO's April 2004 report, resulted in a 2004 DBT that has been refined and more closely identified with the terrorist parameters reflected in the intelligence community's postulated threat. An additional challenge involves the fact that National Nuclear Security Administration (NNSA) has not been fully effective in managing its safeguards and security program. As a result, NNSA has had difficulty in providing fully effective oversight to ensure that its contractors are properly protecting its critical

[21]See GAO, *Nuclear Security: DOE Needs to Resolve Significant Issues before It Fully Meets the New Design Basis Threat*, GAO-04-623 (Washington, D.C.: Apr. 27, 2004).

[22]See GAO, *Nuclear Security: DOE Must Address Significant Issues to Meet the Requirements of the New Design Basis Threat*, GAO-04-701T (Washington, D.C.: Apr. 27, 2004).

facilities and materials from individuals seeking to inflict damage.[23] Finally, although both DOE and NNSA have made progress in implementing security initiatives, both agencies could benefit from clarifying the roles and authorities of various security offices and developing methods for evaluating program effectiveness and improvement.[24]

## Improving Security at DOD Installations

The homeland security strategy discusses critical infrastructure as "those systems and assets so vital to the United States that their destruction or incapacity would have a debilitating impact on security." As DOD installations are an essential element of the national defense establishment, it follows that their security is equally essential. However, we have found that DOD faces challenges in safeguarding its installations and personnel from terrorist attacks. Specifically, in August 2004,[25] we reported that although DOD has taken several steps and committed significant resources to immediately begin installation preparedness improvements, it lacks a comprehensive approach that incorporates results-oriented management principles to guide improvement initiatives in the most efficient and effective manner. A major challenge DOD faces is the lack of a single organization or entity with the responsibility and authority to integrate and manage the installation preparedness improvement efforts of numerous DOD organizations engaged in efforts to improve installation preparedness. Additional challenges to be overcome include DOD's difficulty in developing departmentwide standards and

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

[24]GAO, *Nuclear Security: Lessons to Be Learned from Implementing NNSA's Security Enhancements*, GAO-02-358 (Washington, D.C.: Mar. 29, 2002).

[25]GAO, *Combating Terrorism: DOD Efforts to Improve Installation Preparedness Can Be Enhanced with Clarified Responsibilities and Comprehensive Planning*, GAO-04-855 (Washington, D.C.: Aug. 12, 2004).

concepts of operations for installation preparedness and in preparing a comprehensive plan for installation preparedness.

# Appendix VI: Defending Against Catastrophic Threats

This appendix sets forth the definition and major initiatives of the Defending Against Catastrophic Threats mission area and discusses the agencies with major roles, their funding, the alignment of their strategic plans and implementation activities with the major initiatives, and a summary of the challenges faced by the nation. This appendix presents baseline information that can be used by Congress to provide oversight and track accountability for the initiatives in the Defending Against Catastrophic Threats mission area.

## Definition and Major Initiatives

The *National Strategy for Homeland Security* categorizes homeland security activities into six mission areas, the fifth of which is Defending Against Catastrophic Threats. This mission area includes homeland security programs that involve protecting against, detecting, deterring, or mitigating terrorist use of weapons of mass destruction, including understanding terrorists' efforts to gain access to the expertise, technology, and materials needed to build chemical, biological, radiological, and nuclear (CBRN) weapons. In addition, this mission area includes planning and activities related to decontaminating buildings, facilities, or geographic areas after a catastrophic event. This mission area dovetails into Border and Transportation Security, Critical Infrastructure Protection, and Emergency Preparedness and Response as detection technologies are fielded and integrated into broader processes.[1] Figure 11 shows an example of the type of activities carried out in the Defending Against Catastrophic Threats mission area.

The strategy identifies the following major initiatives in the Defending Against Catastrophic Threats mission area:

- preventing terrorist use of nuclear weapons through better sensors and procedures;
- detecting chemical and biological materials and attacks;
- improving chemical sensors and decontamination techniques;
- developing broad-spectrum vaccines, antimicrobials, and antidotes;
- harnessing the scientific knowledge and tools to counter terrorism; and
- implementing the Select Agent Program.

[1]This definition is from OMB's *2003 Report to Congress on Combating Terrorism* (Washington, D.C.: Sept. 2003).

**Figure 11: First Responders Practice Emergency Decontamination**

Source: GAO.

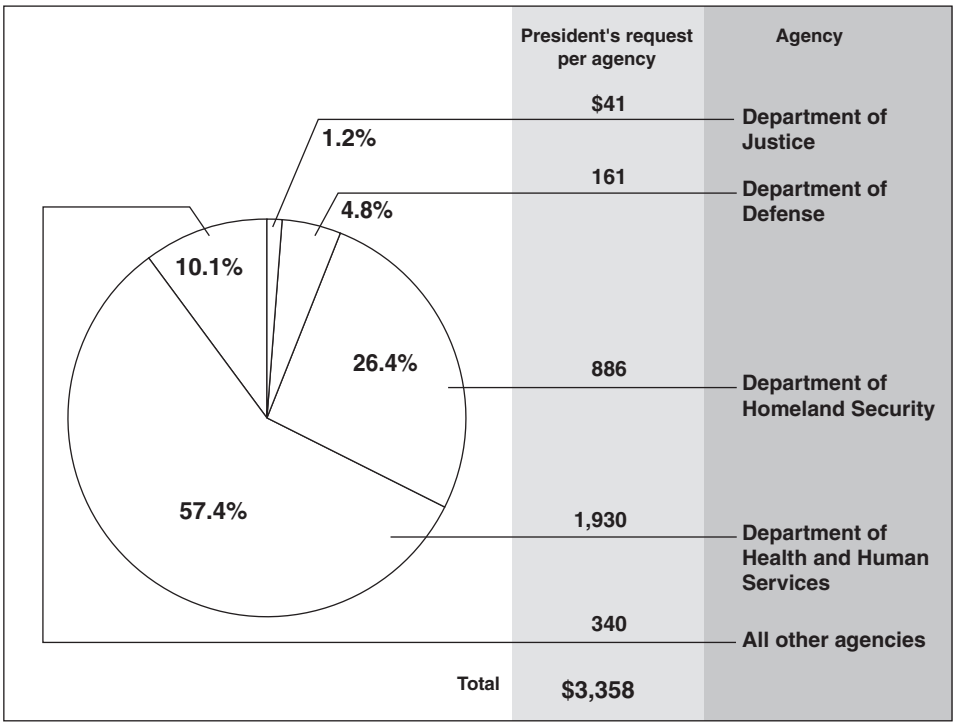
## Agencies with Major Roles in Defending against Catastrophic Threats

Of the six departments under review, DHS and HHS have major roles in Defending Against Catastrophic Threats. DHS's Science and Technology Directorate develops and tests technologies and systems to detect CBRN materials and high explosives, develops and tests forensic methods to analyze CBRN materials and high explosives, and prioritizes measures to address catastrophic threats through research and modeling. HHS's National Institutes of Health (NIH) conducts basic and applied research related to likely bioterrorism agents; designs and tests diagnostics, therapies, and vaccines; and maintains laboratory capacity and provides expert assistance to address bioterrorism and other threats. Other organizations involved in this mission area include DOD, which performs research and development related to chemical and biological threats; the Department of Commerce, which is working to improve export control of weapons, materials that may be used to construct weapons, and other technologies; and the National Science Foundation, which is working to improve security and control of nuclear fuels.

OMB reported that the total 2005 funding request for Defending Against Catastrophic Threats is just over $3.3 billion. The agencies with the most

funding are HHS ($1.9 billion, or 57 percent), largely for research at NIH, and in DHS's Directorate of Science and Technology ($886 million, or 26 percent).[2] Figure 12 summarizes the fiscal year 2005 budget request for the Defending against Catastrophic Threats mission area by agency.

**Figure 12: Proposed Fiscal Year 2005 Homeland Security Funding for Defending Against Catastrophic Threats**




Source: GAO, based on OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005.*

Notes: Budget authority in millions of dollars.

"All other agencies" includes USDA ($227 million) and the Department of Commerce ($66 million) as well as the National Science Foundation ($27 million) and the Nuclear Regulatory Commission ($16 million).

OMB's reported data do not include funding for two departments that have activities under way in this mission area. These departments—DOE and State—have either planning or implementation activity on specific

[2]OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005* (Washington, D.C.: Feb. 2004).

initiatives, as discussed in the next section of this appendix. On the basis of our previous work, we have noted several qualifications to OMB's figures to explain this discrepancy.[3] According to OMB officials, there is not always a clear distinction between homeland security activities and other related activities. OMB staff must make judgment calls about how to characterize funding by mission areas. For example, some homeland security activities have multiple purposes and funding for these activities is allocated to different accounts that can cover multiple mission areas. In addition, some of the departments' activities, such as planning, coordination, or providing advice may support Defending Against Catastrophic Defense activities but are not included in the amounts shown.

## Alignment of Department Activities with the Major Initiatives

In this section, we provide more detailed information about the Defending Against Catastrophic Threats mission area initiatives and the departments involved in conducting activities related to these initiatives. This includes a discussion of specific departmental planning/implementation activities, agency leads, and implementation activities during fiscal year 2004, with respect to each initiative. The data are summarized in table 11.

[3]See GAO, *Combating Terrorism: Funding Data Reported to Congress Should be Improved*, GAO-03-170 (Washington, D.C.: Nov. 26, 2002).

**Table 11: Detailed Department Planning/Implementation Activities in the Defending Against Catastrophic Threats Mission Area's Six Initiatives**

| | DHS | | | DOJ | | | DOD | | | HHS | | | State | | | DOE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 |
| **Defending against catastrophic threats** | | | | | | | | | | | | | | | | | | |
| (1) Prevent terrorist use of nuclear weapons through better sensors and procedures | ● | ● | ● | | | | ● | ● | ● | | | | ● | ● | ● | ● | ● | ● |
| (2) Detect chemical and biological materials and attacks | | ● | ● | | | | ● | ● | | ● | ● | ● | | | | ● | ● | ● |
| (3) Improve chemical sensors and decontamination techniques | | ● | ● | | | | | | | ● | ● | ● | | | | ● | ● | ● |
| (4) Develop broad spectrum vaccines, antimicrobials, and antidotes | | ● | ● | | | | | | | | ● | ● | ● | ● | ● | ● | | ● |
| (5) Harness the scientific knowledge and tools to counter terrorism | ● | ● | ● | | | | ● | | | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| (6) Implement the Select Agent program | | | | | | | ● | | | ● | ● | ● | | | | | | |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Department IMPLICITLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

PI = Prior implementation to fiscal year 2004
RP = Recent planning
04 = Fiscal year 2004 implementation

Source: GAO.

## Summary of Departmental Activities on the Initiatives

All six Defending Against Catastrophic Threats initiatives are being addressed in key departments' planning and implementation activities. As shown in table 11, at least two departments cited activity in each of the six initiatives. At least four departments cited activity in four of the six initiatives. For example, DHS, DOD, State, and DOE implemented activities in fiscal year 2004 to prevent terrorist use of nuclear weapons through better sensors and procedures. DHS's Science and Technology Directorate provided leadership in directing, funding, and coordinating research, development, testing, and evaluation and procurement of technology and systems to prevent the importation of chemical, biological, and radiological nuclear and related weapons; DOD activities addressed the clandestine transportation of weapons of mass destruction, including nuclear devices, via the Container Security and Proliferation Security Initiatives; State pursued diplomatic efforts in fiscal year 2004 to ensure compliance with existing multilateral treaties, strengthening verification and compliance procedures, and strengthening the International Atomic Energy Agency; and DOE worked with DOD to secure Iraqi radiological

and nuclear materials, as well as continued research at Los Alamos National Laboratory on radiological and nuclear countermeasures. Additionally, DHS, DOE, and HHS demonstrated fiscal year 2004 implementation activities oriented toward improving chemical sensors and decontamination techniques. With regard to sensors, DHS's Homeland Security Advanced Research Projects Agency approved multiple chemical sensor technology contracts, and HHS continued to increase the number of toxic substances that can be readily measured by Rapid Toxic Screen testing. With regard to decontamination, DOE, through a national laboratory, developed a decontamination countermeasure for biological and chemical agents.

The only department that did not have activities related to Defending Against Catastrophic Threats initiatives is DOJ. This is understandable, given that Justice is concerned with identifying, capturing, and prosecuting individuals involved in terrorist activity rather than developing and improving sensors, vaccines, antimicrobials, antidotes, and decontamination techniques and procedures.

## Identification of Lead Agencies in the Initiatives

For all six initiatives, a lead agency is identified either in the strategy or HSPDs. As shown in table 11, DHS is a lead on all six initiatives. It seems appropriate that DHS would be the department with the most leads, given that the strategy's "national vision" calls for that department to "unify much of the federal government's efforts to develop and implement scientific and technological counter-measures against human, animal, and plant diseases that could be used as terrorist weapons" and "sponsor and establish national priorities for research, development, and testing to develop new vaccines, antidotes, diagnostics, therapies and other technologies against chemical, biological, radiological, or nuclear terrorism." HHS is also a lead on two initiatives, both oriented toward the public health safety of the nation (improving chemical sensors and decontamination techniques and developing broad spectrum vaccines, antimicrobials, and antidotes). More specifically, DOD, State, and DOE are all leads on the same single initiative (preventing terrorist use of nuclear weapons through better sensors and procedures).

The strategy and HSPDs identified multiple leads on three of the six Defending Against Catastrophic Threats initiatives (see table 11). DHS, DOD, State, and DOE are all leads on one initiative, preventing terrorist use of weapons through better sensors and procedures; and DHS and HHS are both leads on two initiatives (improving chemical sensors and decontamination techniques and developing broad-spectrum vaccines,

antimicrobials, and antidotes.) More specifically, with respect to the latter initiative, DHS identifies needs and coordinates activities rather than actually developing the vaccines, antimicrobials, and antidotes. The initiative is broadly defined to cover each of these areas. In addition, departmental strategic planning and implementation documents show that DHS is a clear lead on four of the six initiatives; and DOD, HHS, State, and DOE are implied leads on all their initiatives.

## Fiscal Year 2004 Implementation of the Initiatives

In fiscal year 2004, implementation activity occurred with respect to all six of the Defending Against Catastrophic Threats initiatives (see table 11). DHS implemented activity in five of the six initiatives for which it was identified as a lead by either the strategy or HSPDs. HHS implemented activity in both initiatives for which it was identified as a lead; State, DOD, and DOE each implemented activity in the single initiative for which they are leads.

Additionally, several of the departments under review implemented multiple Defending Against Catastrophic Threats initiatives for which they were not identified as a lead in the strategy or HSPDs. During fiscal year 2004, HHS and DOE cited implementation activities (as well as prior implementation activities) in three and four initiatives, respectively, for which they were not a lead; State cited implementation and prior implementation activities in two initiatives for which it was not a lead. DOD conducted prior implementation activities in three initiatives for which it was not a lead.

In accordance with the Homeland Security Act of 2002, several departments transferred some of their programs and centers to the newly created DHS. In the case of DOE, the nuclear smuggling programs and activities that had previously been within the proliferation detection program were transferred to DHS; DOE's chemical and biological national security and supporting programs were transferred; activities of the nonproliferation and verification research and development program and nuclear activities associated with assessment, detection, and cooperation regarding international materials and protection were all transferred to DHS. In the case of DOD, functions of the National Bio-Weapons Defense Analysis Center, including related functions of the Secretary of Defense, were also transferred to DHS.

## Challenges in Defending Against Catastrophic Threats

The expertise, technology, and material needed to build the most deadly weapons known to mankind—including chemical, biological, radiological, and nuclear weapons—are proliferating. The consequences of a terrorist attack using these types of weapons could be far more devastating than those suffered on September 11, in that such an attack could cause a large numbers of casualties, mass psychological disruption, and widespread contamination, and could overwhelm local medical capabilities. Our recent work in the Defending Against Catastrophic Threats mission area has identified a number of challenges. These challenges include the strengthening of efforts involving the nonproliferation of weapons of mass destruction, dangerous weapons systems and materials, and dual-use items; the control of the sale of excess items that can be used to produce and deliver biological agents; and the designation of lead agencies for setting priorities for information systems related to bioterrorism.

## Strengthening Nonproliferation Efforts

The strategy declares that one of the nation's top priorities is to keep weapons of mass destruction out of the hands of terrorists. We have issued a number of reports concerning U.S. efforts to more effectively control and limit the spread of weapons of mass destruction, dangerous weapons systems and materials, and dual-use items. United States efforts in this regard are designed to prevent sensitive items from reaching persons, entities, or countries involved in terrorism or the proliferation of weapons of mass destruction and the vehicles to deliver them.

We testified in March 2004 that the Departments of Commerce (Commerce), State, and Defense need to enhance their programs in this area.[4] Specifically, we found that the United States faces a growing threat from the international proliferation of cruise missile and unmanned aerial vehicle (UAV) technology, challenging the tools the U.S. government has traditionally used. Multilateral export control regimes have expanded their lists of controlled items, but key countries of concern are not members. Some of these countries are also on the State Department's list of state sponsors of terrorism. In addition, U.S. efforts to control U.S. exports of dual-use items are hindered by a gap in U.S. export control authority. U.S. companies can sell certain dual-use items to foreign buyers, even if the exporter knows the buyer plans to use the items to build cruise missiles or UAVs. Finally, the United States seldom uses its end-use monitoring

[4]See GAO, *Nonproliferation: Improvements Needed for Controls on Exports of Cruise Missiles and Unmanned Aerial Vehicles*, GAO-04-493T (Washington, D.C.: Mar. 9, 2004).

program to verify compliance with conditions placed on the use of cruise missiles.

With regard to export controls over items that could be employed by terrorists, we found that post-shipment verification (PSV) provides limited assurance that dual-use items are being properly used. Specifically, we reviewed Commerce's efforts to conduct PSV checks to ensure that dual-use items and technologies arrive at their intended destination and are used for the purpose stated in the export license. We reported, in February 2004,[5] that Commerce conducted relatively few post-shipment verification checks. For example, PSV checks were completed on only 6 percent of dual-use items exported to countries of potential proliferation concern. We also identified three key challenges in the PSV process itself. First, PSVs do not confirm compliance license conditions because U.S. officials frequently do not check license compliance, they often lack the technical training to assess compliance, and end-users may not be aware of the license conditions they are supposed to be abiding by. Second, some countries of concern limit the U.S. government's access. Third, PSV results have only limited impact on Commerce's future licensing decisions. Commerce generally agreed with our recommendation to address these challenges and indicated it had taken steps to strengthen the PSV process.

In March 2004,[6] we reported that another area of proliferation raising potential terrorism concerns involves delays in implementing the Chemical Weapons Convention (CWC). CWC bans chemical weapons and requires their destruction by 2007, with possible extension to 2012. CWC has played an important role in reducing the risks posed by chemical weapons. However, CWC's nonproliferation goals have proven more challenging than originally anticipated. First, the destruction of chemical weapons will likely take longer and cost more than originally anticipated. Even with significant international assistance, Russia may not be able to destroy its declared chemical weapons stockpile until 15 years beyond the extended CWC deadline. Second, technical advancements in the chemical industry and the increasing number of dual-use commercial facilities worldwide challenge the CWC's ability to deter and detect proliferation. Third, many CWC member states have not yet adopted national laws to

[5]See GAO, *Export Controls: Post-Shipment Verification Provides Limited Assurance That Dual-Use Items Are Being Properly Used*, GAO-04-357 (Washington, D.C.: Feb. 11, 2004).

[6]See GAO, *Delays in Implementing the Chemical Weapons Convention Raise Concerns about Proliferation*, GAO-04-361 (Washington, D.C.: Mar. 31, 2004).

fully implement the CWC or have not submitted complete and accurate declarations of their CWC-related activities.

The Bremer, Gilmore, Hart-Rudman, and 9/11 commissions made recommendations related to the challenges presented in this section.

## Controlling the Sale of Biological Production Equipment

Another challenge related to keeping weapons of mass destruction out of the hands of terrorists involves the ability of terrorists to readily obtain equipment that can be used to make biological agents. We have previously reported[7] that many items needed to establish a laboratory for making biological warfare agents were being sold on the Internet to the public from DOD's excess property inventory for pennies on the dollar—making them both easy and economical to obtain. Although production of biological warfare agents requires a high degree of expertise, public sales of these DOD excess items increase the risk that terrorists could obtain and use them to produce and deliver biological agents within the United States. To prove this point, we created a fictitious company and purchased over the Internet key excess DOD biological equipment items and related protective clothing necessary to produce and disseminate biological warfare agents. Additionally, our investigation of several buyers of the biological equipment items found that they exported them to countries, such as the Philippines, Egypt, and the United Arab Emirates, for transshipment to other countries—some of which may be prohibited from receiving exports of similar trade-security-controlled items. Finally, the possibility that anthrax and other biological agents could have fallen into the wrong hands because of poor controls at laboratories handling biological agents calls for an assessment of the challenge to national security posed by public sales of excess biological laboratory equipment and protective clothing. While it should be noted that our work to date has focused on DOD sales, we found that these same types of items are available from other sources, indicating a much broader problem. The Bremer, Gilmore, Hart-Rudman, and 9/11 Commissions made recommendations related to this challenge.

[7]See GAO, *DOD Excess Property: Risk Assessment Needed on Public Sales of Equipment That Could Be Used to Make Biological Agents*, GAO-04-15NI (Washington, D.C.: Nov. 19, 2003).

## Effective Implementation of Emerging Information Technologies

The strategy calls for the development of a national system to detect biological and chemical attacks that will include "a public health surveillance system to monitor public and private databases for indicators of biological or chemical attack." One of the challenges we identified in a May 2003 report[8] is that there are six federal agencies with key roles in bioterrorism preparedness and response. Within these six agencies, we identified 72 information systems and supporting technologies, as well as 12 other information technology initiatives, with about 74 percent of these currently operational. Of the 72 information systems identified, 34 are surveillance systems, 18 are supporting technologies, 10 are communication systems, and 10 are detection systems. In planning or operating each of these information systems and IT initiatives, the extent of coordination or interaction among the lead and other related government agencies covered a wide range. There was no one entity or coordinating body to set priorities for information systems, supporting technologies, and other IT initiatives.

Within the public health sector, the implementation of emerging information technologies could help to strengthen agencies' technological capabilities to support the nation's ability to prepare for and respond to bioterrorism and other public health emergencies. Agencies identified several activities to research, develop, and implement emerging technologies, and these activities are generally initiated to meet agencies' specific needs. However, challenges exist that may hinder the public health community from benefiting from the implementation of emerging information technologies. These challenges include (1) the likelihood that emerging technologies have not been in use long enough for the developers to identify all areas of standardization, or for the technologies to have evolved to the point that they are interoperable with other existing technologies within public health; (2) the likelihood that the use of emerging technologies may change an organization's existing business model and thereby introduce a significant level of risk by disrupting existing business practices; and (3) the lack of a clearly defined mechanism for continuing research and development for emerging technologies once the results are turned over to the public sector.

[8]See GAO, *Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies*, GAO-03-139 (Washington, D.C.: May 30, 2003).

The Gilmore Commission made recommendations with regard to this challenge.

## Safeguarding Military Installations

As DOD installations are an essential element of the nation's national defense establishment, it follows that their security is equally essential. However, we reported in August 2004 that DOD faces challenges in safeguarding its installations and personnel in the United States and overseas from terrorist attacks involving chemical, biological, radiological, and nuclear weapons and high explosives.[9] Specifically, we found that improving the preparedness of military installations is a challenging and complex task that will require a significant allocation of resources; involve numerous organizations within the department; and necessitate the coordination with other federal agencies, civilian organizations, and foreign host governments. Although DOD has taken several steps and committed significant resources to immediately begin installation preparedness improvements, it faces significant challenges and lacks a comprehensive approach that incorporates results-oriented management principles to guide improvement initiatives in the most efficient and effective manner. One major challenge DOD faces is the lack of a single organization or entity with the responsibility and authority to oversee and integrate the installation preparedness improvement efforts of various DOD organizations. Additional challenges to be overcome include the evolving or unclear responsibilities of key organizations and assignment of responsibility to update DOD's installation preparedness plans.

[9]See GAO-04-855.

# Appendix VII: Emergency Preparedness and Response

This appendix sets forth the definition and major initiatives of the Emergency Preparedness and Response mission area and discusses the agencies with major roles, their funding, the alignment of their strategic plans and implementation activities with the major initiatives, and a summary of the challenges faced by the nation. This appendix presents baseline information that can be used by Congress to provide oversight and track accountability for the initiatives in the Emergency Preparedness and Response mission area.

## Definition and Major Initiatives

The *National Strategy for Homeland Security* categorizes homeland security activities into six mission areas, the sixth of which is Emergency Preparedness and Response. This mission area includes programs that prepare to minimize the damage and recover from any future terrorist attacks that may occur despite our best efforts at prevention. Included here are programs that help to plan, equip, train, and practice the needed skills of the varied and necessary first responders—including police officers, firefighters, emergency medical providers, public works personnel, and emergency management officials. Finally, this mission area includes activities to consolidate federal response plans and activities to build a national system for incident management in cooperation with state and local government.[1] Figure 13 shows an example of the types of activities carried out in the Emergency Preparedness and Response mission area.

The strategy identifies the following major initiatives in the Emergency Preparedness and Response mission area:

- integrating separate federal response plans into a single all-discipline incident management plan;
- creating a national incident management system;
- improving tactical counterterrorist capabilities;
- enabling seamless communication among all responders;
- preparing health care providers for catastrophic terrorism;
- augmenting America's pharmaceutical and vaccine stockpiles;
- preparing for chemical, biological, radiological, and nuclear decontamination;
- planning for military support to civil authorities;
- building the Citizen Corps;

[1]This definition is from OMB's *2003 Report to Congress on Combating Terrorism* (Washington, D.C.: Sept. 2003).

- implementing the first responder initiative of the fiscal year 2003 budget;
- building a national training and evaluation system; and
- enhancing the victim support system.

**Figure 13: Hazardous Materials Response Unit in Action at an Exercise**


Source: GAO.

## Agencies with Major Roles in Emergency Preparedness and Response

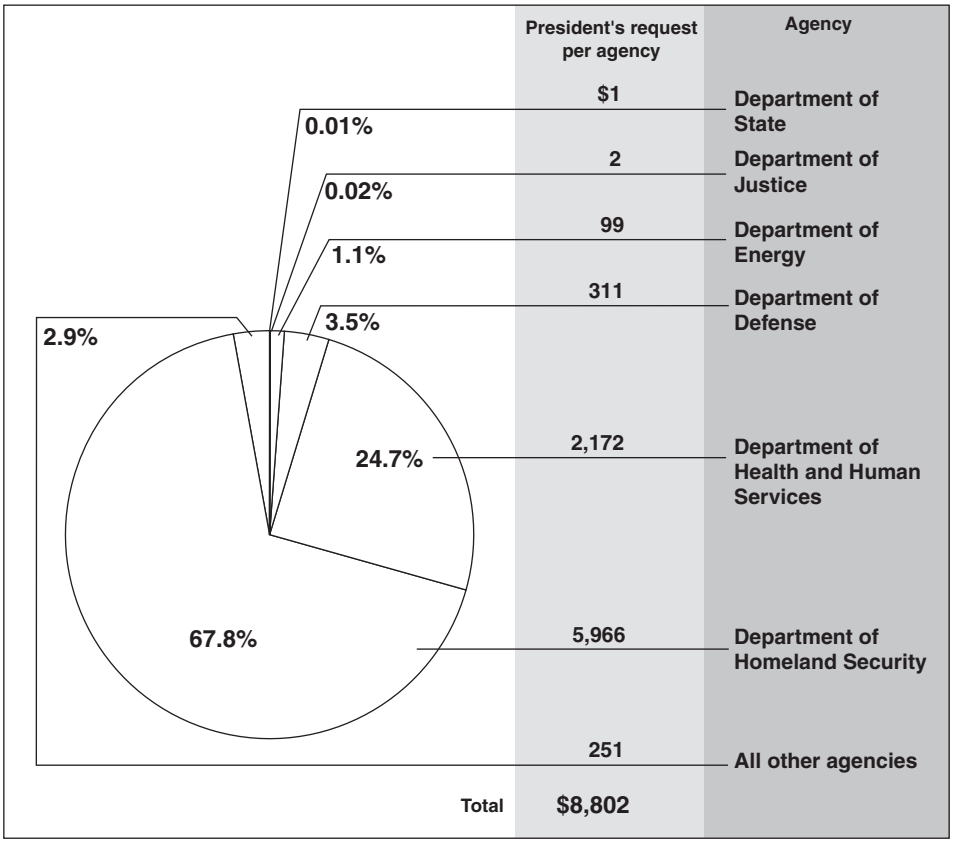
Of the six departments under review, the Department of Homeland Security and the Department of Health and Human Services have major roles in Emergency Preparedness and Response. DHS's activities include the development and implementation of the National Response Plan and the National Incident Management System, maintaining the National Disaster Medical System and Urban Search and Rescue Teams, and supporting state and local first responders through a wide-range of programs. HHS's activities are centered on preparing the nation's health care providers for catastrophic terrorism by, among other things, maintaining the Strategic National Stockpile and other emergency preparedness and response assets. In addition to DHS and HHS, several other agencies—including the Department of Defense, which maintains weapons of mass destruction (WMD) response teams to support civil authorities; and the Department of Energy, which maintains radiological and nuclear response capabilities—are involved in Emergency Preparedness and Response.

The Office of Management and Budget reported that the total fiscal year 2005 funding request for the Emergency Preparedness and Response mission area is just over $8.8 billion. DHS receives the largest share of this funding ($5.9 billion, or 68 percent), mostly for preparedness and grant assistance to state and local first responders and Project Bioshield. HHS also receives a significant amount of this funding ($2.2 billion, or 25 percent) for assisting states and localities in upgrading their public health capacity. A total of 18 other federal agencies receive emergency preparedness and response funding, with a number of these maintaining specialized response assets that may be called upon in select circumstances.[2] Examples of these agencies include DOD, which maintains WMD response teams to support civil authorities; DOE, which maintains radiological and nuclear response capabilities; and the Environmental Protection Agency, which maintains chemical, biological, radiological, and nuclear response teams.[3] Figure 14 summarizes the fiscal year 2005 budget request for the emergency preparedness and response mission area by agency.

[2]OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005* (Washington, D.C.: Feb. 2004).

[3]OMB, *2003 Report to Congress on Combating Terrorism* (Washington, D.C.: Sept. 2003).

**Figure 14: Proposed Fiscal Year 2005 Homeland Security Funding for Emergency Preparedness**




Source: GAO, based on OMB, *Analytical Perspectives, Budget of the United States Government, Fiscal Year 2005.*

Notes: Budget authority in millions of dollars.

" All other agencies" includes the Departments of Agriculture ($69 million), Veterans Affairs ($33 million), Commerce ($25 million), Treasury ($16 million), Transportation ($14 million), Labor ($10 million), Interior ($4 million) and Education ($1 million), as well as EPA ($30 million), and several others.

## Alignment of Department Activities with the Major Initiatives

This section provides more detailed information about the Emergency Preparedness and Response mission area initiatives and the departments involved in conducting activities related to these initiatives. This includes a discussion of specific departmental planning/implementation activities, lead agency designations, and department implementation activities in fiscal year 2004, with respect to each initiative. The data are summarized in table 12.

**Table 12: Detailed Department Planning/Implementation Activities in the Emergency Preparedness and Response Mission Area's Twelve Initiatives**

| | DHS | | | DOJ | | | DOD | | | HHS | | | State | | | DOE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 |
| **Emergency preparedness and response** | | | | | | | | | | | | | | | | | | |
| (1) Integrate separate federal response plans into a single all-discipline incident management plan | | ● | ● | | | | | ● | ● | | ● | ● | | | | | ● | ● |
| (2) Create a national incident management system | | ● | ● | | | | | ● | | | ● | ● | | | | | ● | ● |
| (3) Improve tactical counter terrorist capabilities | ● | ● | ● | | | | | ● | | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| (4) Enable seamless communication among all responders | | ● | ● | | | | | | | ● | ● | ● | | | | | | |
| (5) Prepare health care providers for catastrophic terrorism | | ● | ● | | | | | ● | ● | ● | ● | ● | | | | | ● | ● |
| (6) Augment America's pharmaceutical and vaccine stockpiles | | ● | ● | | | | | ● | | ● | ● | ● | | | | | ● | ● |
| (7) Prepare for chemical, biological, radiological, and nuclear decontamination | | ● | ● | | | | ● | | ● | | ● | ● | | | | | ● | ● |
| (8) Plan for military support to civil authorities | | | ● | | | | ● | ● | ● | | | | | | | | | |
| (9) Build the Citizen Corps | | ● | ● | | | ● | | | | | | | | | | | | |
| (10) Implement the first responder initiative of the fiscal year 2003 budget | ● | | ● | ● | ● | ● | | | | | | | | | | | | |
| (11) Build a national training and evaluation system | | ● | ● | ● | | | | ● | | | ● | ● | | | | | | |
| (12) Enhance the victim support system | | ● | ● | | | ● | | | | | ● | ● | | | | | | |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Department IMPLICITLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

PI = Prior implementation to fiscal year 2004
RP = Recent planning
04 = Fiscal year 2004 implementation

Source: GAO.

## Summary of Departmental Activities on the Initiatives

All 12 Emergency Preparedness and Response initiatives are being addressed in key departments' planning and implementation activities. As shown in table 12, at least two departments cited activity in each of the 12 initiatives. At least four departments cited activity in 7 of the 12 initiatives. For example, DHS, DOD, HHS, and DOE each cited implementation activities in fiscal year 2004 with respect to creating a national incident management plan. DHS Federal Emergency Management Agency worked on a comprehensive National Incident Management System that

incorporates federal, state, tribal, and local government personnel, agencies, and regional authorities; DOD participated in the planning of the National Incident Management System; HHS issued continuing guidance to assist state and local jurisdictions in preparation for joining the National Incident Management System; and DOE implemented an agreement to release departmental emergency response assets to DHS as requested in support of DHS's national incident management role. Additionally, DHS and HHS implemented activities in fiscal year 2004 toward creating seamless communication among all responders. DHS established an office to oversee interoperability efforts, contracts have been awarded to develop interoperability communication technologies, and the DHS Science and Technology Directorate is leading the RAPIDCOM initiative (under SAFECOM, a federal governmentwide program to achieve communication interoperability), and HHS (through its Centers for Disease Control and Prevention) increased the percentage of health departments with interoperable, redundant communication systems and high-speed Internet access, and has raised the number of jurisdictions having access to the Epidemic Information Exchange.

All departments have implemented several initiatives in fiscal year 2004 related to the Emergency Preparedness and Response critical mission area, with one exception: State has implemented activity with respect to only one initiative (improving tactical counterterrorist capabilities).

## Identification of Lead Agencies on the Initiatives

For all 12 initiatives, a lead agency is identified either in the strategy or the Homeland Security Presidential Directives. DHS is the lead on the most initiatives in this mission area—11 of the 12 initiatives, the single exception being the initiative to augment America's pharmaceutical and vaccine stockpiles. It seems appropriate that DHS would be the department with the most leads given that the strategy's "national vision" calls for DHS to "consolidate federal response plans and build a national system for incident management" and "ensure that leaders at all levels of government have complete incident awareness and can communicate with and command all appropriate response personnel."

Additionally, HHS is a lead on 3 of the 12 initiatives—augmenting America's pharmaceutical and vaccine stockpiles; preparing for chemical, biological, radiological, and nuclear decontamination; and building a national training and evaluation system. DOD is a lead on 1 of the 12 initiatives within this mission area—planning for military support to civil authorities. Three departments have not been identified as a lead on any initiatives in this mission area: DOJ, State, and DOE.

The strategy and HSPDs identified multiple leads on 2 initiatives (see table 12). DHS and DOD are both leads on planning for military support to civil authorities; and DHS and HHS are leads on building a national training and evaluation system. In addition, 10 of the 11 DHS leads are clear, and the single DOD lead is clear. HHS lead is clear with respect to augmenting America's pharmaceutical and vaccine stockpiles and implied with respect to building a normal training and evaluation system and preparing for chemical, biological, radiological, and nuclear decontamination. (We included HHS as an implicit lead on the latter initiative since the department was an implicit lead on the closely related initiative, "improving chemical sensors and decontamination techniques" in the Defending against Catastrophic Threat mission area.)

## Fiscal Year 2004 Implementation of the Initiatives

In fiscal year 2004 implementation activity occurred with respect to each of the 12 Emergency Preparedness and Response initiatives (see table 12). DHS implemented activity in 2004 on all 11 initiatives for which it was identified as a lead. DOD implemented prior and 2004 activities in the one area where it was the lead (planning for military support to civil authorities), and HHS implemented prior and 2004 activities in its two lead areas (augmenting America's pharmaceutical and vaccine stockpiles and building a national training and evaluation system).

Additionally, several of the departments under review implemented multiple Emergency Preparedness and Response initiatives for which they were not identified as a lead in either the strategy or HSPDs. During fiscal year 2004, DHS cited implementation activities in the single initiative for which it was not identified as a lead—augmenting America's pharmaceutical and vaccine stockpiles. HHS cited 2004 implementation activities in 7 initiatives for which it was not a lead. Similarly, DOE cited implementation activities in 6 initiatives for which it was not identified as a lead in the strategies or HSPDs; and DOJ and DOD both cited fiscal year 2004 implementation activities in 3 initiatives for which they were not leads, respectively.

DOJ's role in the Emergency Preparedness and Response mission area has been modified because of program transfers. DOJ's Office of Domestic Preparedness (ODP) had provided grant funding to assist state and local emergency response agencies (with respect to law enforcement, fire, hazardous materials, emergency medical services, emergency management, and public health) to enhance their capabilities to respond to threats posed by terrorist use of weapons of mass destruction. This program was transferred to DHS.

## Challenges in Emergency Preparedness and Response

Our recent work in the Emergency Preparedness and Response mission area has identified a number of challenges that must be overcome if the nation is to effectively minimize the damage and successfully recover from future terrorist attacks that may occur despite its best efforts at preventing them. One challenge involves the adoption of an "all-hazards" approach to emergency preparedness and response. Addressing this challenge would ensure that the nation is better prepared for terrorist events while simultaneously better preparing itself to deal with natural disasters. Another challenge involves providing better governmental planning and coordination with regard to first responder issues. An example of the challenge faced here concerns the National Capital Region (NCR), where there exists no coordinated regionwide plan for first responder priorities. Other challenges with regard to first responders include better preparing them to respond to incidents involving catastrophic terrorism and restructuring the federal grant system. An additional challenge involves improving public health communications and information sharing. An example of this challenge is the lack of a coordinated review process that ensures that communications projects complement one another. Additional challenges include better preparing health care providers to respond to incidents involving bioterrorism; improving regional response planning involving multiple municipalities; ensuring that hospitals have the medical equipment necessary for large influxes of patients; ensuring adequate communications among responders and with the public, and defining the roles and responsibilities of DOD in defending the homeland and providing military support to civil authorities.

## Adopting an All-hazards Approach

The strategy calls for the creation of "a fully integrated national emergency response system that is adaptable enough to deal with any terrorist attack, no matter how unlikely or catastrophic, as well as all manner of natural disasters." This all-hazards approach to emergency preparedness and response has been embodied in a number of documents, including HSPD-5 and HSPD-8; the National Incident Management System; and the National Response Plan. In our May, June, and July 2004 reports,[4] we pointed out

[4]See GAO, *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); *Homeland Security: Coordinated Planning and Standards Needed to Better Manage First Responder Grants in the National Capital Region*, GAO-04-904T (Washington, D.C.: June 24, 2004); and *Homeland Security: Federal Leadership and Intergovernmental Coordination Required to Achieve First Responder Interoperable Communications*, GAO-04-740 (Washington, D.C.: July 20, 2004).

that the challenges the nation's emergency responders face in adapting an all-hazards approach include (1) identifying the types of emergencies—e.g., hurricane or truck bomb attack—for which they should be prepared and the requirements—e.g., incident management plans and procedures, equipment, and training—for responding effectively to these different types of emergencies; (2) assessing current capabilities against those requirements; (3) developing and implementing effective, coordinated plans among multiple first responder disciplines and jurisdictions to close the gap between current capabilities and established requirements; and (4) defining the roles and responsibilities of federal, state, and local governments and private entities in defining requirements, assessing capabilities, and developing and implementing coordinated plans to enhance first responder capabilities. The Gilmore and 9/11 commissions made recommendations with regard to this challenge.

## Improving Intergovernmental Planning and Coordination

The strategy emphasizes a shared national responsibility—involving all levels of government—in responding to a serious emergency, such as a terrorist incident. However, in May 2004 we reported that a major challenge involves a lack of coordination in preparing for, responding to, and recovering from terrorist and other emergency incidents.[5] In particular, our work indicates that there has been a lack of regional planning and coordination for developing first responder preparedness, defining preparedness goals, identifying spending priorities, and expending funds. For example, our review of the first responders grants in the National Capital Region (NCR) found that there was no coordinated regionwide plan for establishing first responder performance goals, needs, and priorities and assessing benefits of expenditures to enhance first responder capabilities. As a result, NCR faces several challenges in organizing and implementing efficient and effective regional preparedness programs, including the lack of a coordinated strategic plan for enhancing NCR preparedness, performance standards, a central source of data on funds available and the purposes for which they are spent.

We found similar challenges related to regional coordination in our April 2003 bioterrorism work.[6] The strategy calls for state and local governments to "sign mutual aid agreements to facilitate cooperation with their

[5]See GAO-04-433.

[6]See GAO, *Bioterrorism: Preparedness Varied across State and Local Jurisdictions*, GAO-03-373 (Washington, D.C.: Apr. 7, 2003).

neighbors in time of emergency." Such agreements are particularly important because although the response to a terrorist incident (such as a bioterrorism attack) would occur at the local level, it could spread across local, state, and even national boundaries. We found that health care officials were challenged by a lack of regional coordination between the states and with neighboring countries. Specifically, states tend to organize their planning on a regional basis, assigning local areas to particular regions within the state. Additionally, we found that border states varied with regard to the intensity of their coordination efforts with Canada and Mexico. The Gilmore, Hart-Rudman, and 9/11 commissions made recommendations with regard to this challenge.

## Overcoming Fragmentation of the Federal Grant System

The strategy acknowledges that the federal grant system for first responders is highly fragmented. In September 2003,[7] we testified that this fragmentation leads to challenges in the coordination and integration of services, as well as in planning at state and local levels. There are many different grant programs that can be used by first responders to address preparedness activities. However, in April 2003,[8] we testified that substantial differences exist in the types of recipients and the allocation methods for grants addressing similar purposes. For example, some grants go directly to local first responders, such as firefighters, while others go to state emergency management agencies or directly to state fire marshals. The allocation methods differ as well—some are formula grants, while others involve discretionary decisions by federal agency officials on a project basis. Grant requirements vary as well. For example, DHS's Assistance to Firefighters Grant has a maintenance of effort requirement, while the State Fire Training Systems Grant has no similar requirement. Several alternatives might be employed to overcome problems fostered by this fragmentation, including consolidating grant programs, establishing performance partnerships between federal agencies and state and local governments, and waiving federal funding restrictions and program requirements. The Gilmore and 9/11 commissions made recommendations with regard to this challenge.

[7]See GAO, *Homeland Security: Reforming Federal Grants to Better Meet Outstanding Needs*, GAO-03-1146T (Washington, D.C.: Sept. 3, 2003).

[8]See GAO, *Federal Assistance: Grant System Continues to Be Highly Fragmented*, GAO-03-718T (Washington, D.C.: Apr. 29, 2003).

## Improving Communications and Information Sharing

The strategy has an initiative to enable seamless communications among all first responders and public health entities. However, in our August and November 2003 reports,[9] we stated that insufficient collaboration among federal, state, and local governments creates a challenge for sharing public health information and developing interoperable communications for first responders. For example, states and cities implemented many initiatives to improve information sharing, but these initiatives were not well coordinated and risked creating partnerships that limited access to information and created duplicative efforts. Another challenge involves the lack of effective, collaborative, interdisciplinary, and intergovernmental planning for interoperable communications. For instance, the federal and state governments lack a coordinated grant review process to ensure that funds are used for communication projects that complement each other and add to overall statewide and national interoperability capacity. Moreover, we testified in April 2004[10] that the Wireless Public Safety Interoperable Communications Program, or SAFECOM, has had very limited progress in achieving communication interoperability among all entities at all levels of government and has not achieved the level of collaboration necessary. Finally, in our October 2002 report[11] on public health preparedness, we reported that challenges exist in ensuring communication among responders and with the public. For example, during the anthrax incidents of 2001, local officials identified communication among responders and with the public as a challenge, both in terms of having the necessary communication channels and in terms of making the necessary information available for distribution. The 9/11 Commission made recommendations with regard to this challenge.

[9]See GAO, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760, (Washington, D.C.: Aug. 27, 2003); and *Homeland Security: Challenges in Achieving Interoperable Communications for First Responders*, GAO-04-231 (Washington, D.C.: Nov. 6, 2003).

[10]See GAO, *Project SAFECOM: Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration*, GAO-04-494 (Washington, D.C.: Apr.16, 2004).

[11]See GAO, *Bioterrorism: Public Health Response to Anthrax Incidents of 2001*, GAO-04-152 (Washington, D.C.: Oct. 15, 2003).

## Better Preparing Health Care Providers for Catastrophic Terrorism

The strategy has an initiative to "prepare health care providers for catastrophic terrorism." However, in April 2003,[12] we reported that many local areas and their supporting agencies may not be adequately prepared to respond to such an event. Specifically, while many state and local officials reported varying levels of preparedness to respond to a bioterrorist attack, they reported that challenges existed because of deficiencies in capacity, communication, and coordination elements essential to preparedness and response (such as workforce shortages, inadequacies in disease surveillance and laboratory systems, and a lack of regional coordination and compatible communications systems). Some of these challenges, such as those involving coordination efforts and communication systems, were being addressed more readily, whereas others, such as infrastructure and workforce issues, were more resource-intensive and, therefore, more difficult to address. Generally, we found that cities with more experience in dealing with public health emergencies were generally better prepared for a bioterrorist attack than other cities, although challenges remain in every city. An additional challenge reported to us by state and local officials concerned the lack of adequate guidance from the federal government on what it means to be prepared for bioterrorism. These officials said that they needed specific standards (such as how large an area a response team should be responsible for) to indicate what they should be doing to be adequately prepared. Finally, state officials indicated that a challenge to be overcome involved the lack of sharing of best practices information. These officials stated that while each jurisdiction might need to adapt procedures to its own circumstances, time could be saved and needless duplication of effort avoided if better mechanisms existed for sharing strategies across jurisdictions. The Gilmore, Hart-Rudman, and 9/11 commissions made recommendations with regard to this challenge.

## Improving Response Capabilities

The strategy recognizes that "a major act of biological terrorism would almost certainly overwhelm existing state, local, and privately owned health care capabilities." In fact, in May 2003 we testified that while the efforts of public health agencies and health care organizations to increase their preparedness for major public health threats has increased, significant challenges remain.[13] Specifically, we found that there are gaps

[12]See GAO-03-373.

[13]See GAO, *SARS Outbreak: Improvements to Public Health Capacity Are Needed for Responding to Bioterrorism and Emerging Infectious Diseases*, GAO-03-769T (Washington, D.C.: May 7, 2003).

in disease surveillance systems and laboratory capacity, and the number of personnel trained for disease detection is insufficient. Additionally, most emergency departments across the country lack the capacity to respond to large-scale infectious disease outbreaks. For example, although most hospitals across the country reported participating in basic planning activities for large-scale infectious disease outbreaks, few have acquired the medical equipment resources—such as ventilators—that would be required in such an event. Further, because most emergency departments already routinely experience some degree of overcrowding, they may not be able to handle the sudden influx of patients that would occur during a large-scale terrorist incident or infectious disease outbreak. The Gilmore Commission made recommendations with regard to this challenge.

## Adequately Equipping Hospitals for Large Influxes of Patients

The strategy states that DHS, working with HHS and VA, will help hospitals "expand their surge capacity to care for large numbers of patients in a mass-casualty incident." However, in August 2003 we reported[14] that a challenge to be overcome involved the fact that the medical equipment available for response to such an incident varies greatly among hospitals. Additionally, many hospitals reported that they did not have the capacity to respond to the large increase in the number of patients that would be likely to result from a bioterrorist incident with mass casualties. For example, if a large number of patients with severe respiratory problems associated with anthrax or botulism were to arrive at a hospital, a comparable number of ventilators would be required to treat them. However, half of the hospitals we reviewed had, per 100 staffed beds, fewer than six ventilators, three or fewer personal protective equipment suites, fewer than four isolation beds, or the ability to handle fewer than six patients per hour through a 5-minute decontamination shower. Overcoming this challenge is particularly difficult because bioterrorism preparedness is expensive, and hospitals are reluctant to create capacity that is not needed on a routine basis and may never be needed at a particular facility. Related to this challenge, HSPD-10 stated that HHS "in coordination with other appropriate federal departments and agencies, is the principal federal agency responsible for coordinating all federal-level assets activated to support and augment the state and local

[14]See GAO, *Hospital Preparedness: Most Urban Hospitals Have Emergency Plans but Lack Certain Capacities for Bioterrorism Response*, GAO-03-924 (Washington, D.C.: Aug. 6, 2003).

medical and public health response to mass casualty events." The Gilmore Commission made recommendations with regard to this challenge.

## Establishing Emergency Preparedness Standards

Although the strategy discusses benchmarks, standards, and other performance measures for emergency preparedness, we have found that there is not yet a comprehensive set of preparedness standards for assessing first responder capacities, identifying gaps in those capacities, and measuring progress in achieving performance goals. Additionally, in June 2004, we testified[15] that state and local officials were concerned about the lack of specific standards for determining preparedness, and these officials noted that specific benchmarks would help them determine whether they were adequately prepared to respond to a bioterrorism incident. Moreover, in our past work on interoperable communications,[16] we discussed the need to establish national interoperability performance goals and standards. Finally, we have reported on the lack of reliable information on existing federal, state, and local capabilities for combating terrorism and the need to develop a comprehensive inventory of existing capabilities. Without standards linked to such capabilities, it will be a challenge to assess preparedness gaps and efforts to address the gaps without information on existing capabilities. The Gilmore Commission made recommendations with regard to this challenge.

## Defining DOD's Homeland Security Roles and Missions

The strategy called for a review of the authority for military assistance in domestic security. One of the reasons for this review is that federal law places some restrictions on military personnel performing law enforcement functions with the United States—functions that might be needed in a terrorist incident.[17] Another reason for this review is that DOD's primary mission is to deter and prevent aggression abroad and fight to win if these measures fail. This is accomplished through military presence and power projection. However, the federal government's view

[15]See GAO, *Homeland Security: Coordinated Planning and Standards Needed to Better Manage First Responder Grants in the National Capital Region*, GAO-04-904T (Washington, D.C.: June 24, 2004).

[16]See GAO-04-231T.

[17] The 1878 Posse Comitatus Act prohibits the direct use of federal military troops in domestic civilian law enforcement, except where authorized by the Constitution or acts of Congress. Congress has expressly authorized the use of the military in certain situations such as to assist with terrorist incidents involving weapons of mass destruction.

of the defense of U.S. territory has changed since September 11. As a result, DOD has adjusted its strategic and operational focus to encompass not only traditional military concerns posed by hostile states overseas but also asymmetric threats directed at our homeland by both terrorists and hostile states. In a July 2003 report,[18] we noted that DOD faces challenges in balancing its domestic and overseas missions with a renewed emphasis on homeland defense. Moreover, current operations both home and abroad are stressing military forces, as shown in personnel tempo data. Complicating the situation is the fact that some units are not well structured for their domestic missions, cannot practice the varied skills needed to maintain combat proficiency while performing domestic missions, and receive little training value from their assigned domestic duties. Therefore military force readiness may erode and future personnel retention problems may develop, if action is not taken to address these challenges. The Gilmore and 9/11 commissions made recommendations with regard to this challenge.

[18]See GAO, *Homeland Defense: DOD Needs to Assess the Structure of U.S. Forces for Domestic Military Missions*, GAO-03-670 (Washington, D.C.: July 11, 2003).

# Appendix VIII: Crosscutting Issues

This appendix describes challenges in implementing the *National Strategy for Homeland Security* that are crosscutting—they cut across the six critical mission areas. Many of them also cut across the federal, state, local and private sectors. Because this appendix is not based on any critical mission area (as defined in the strategy), it does not include information on major initiatives, agencies with major roles, funding by department, or alignment of department plans with major initiatives.

## Crosscutting Challenges

Our recent work has identified a number of challenges to ensuring the security of the homeland that are not confined to a specific mission area. These challenges are governmentwide in nature and include balancing homeland security funding needs with other national requirements, providing timely and transparent homeland security funding information, improving risk management methods for resource allocation and investments, expanding agency use of performance measures that link costs to outcomes, establishing baseline performance goals and measures upon which to assess and improve preparedness, developing and implementing national standards, clarifying roles and responsibilities within and between the levels of government and the private sector, developing a national enterprise architecture, and improving information technology management governmentwide.

In addition to the challenges discussed above, DHS—as the department most responsible for Homeland Security—faces a number of other challenges. Because of this, in January 2003 we designated the overall implementation and transformation of DHS as high-risk.[1] We gave it this designation for three reasons. First, the size and complexity of the effort make the challenge especially daunting, requiring sustained attention and time to achieve the department's mission in an effective and efficient manner. Second, the components being merged into DHS already face a wide array of existing challenges that must be addressed. Finally, if DHS cannot effectively carry out its mission, it exposes the nation to potentially very serious consequences. We are currently in the process of reviewing the challenges faced by DHS, the progress it has made in addressing these challenges, and its continued high-risk designation. The results of this review will be published in a forthcoming GAO report.

[1]See GAO, *Major Management Challenges and Program Risks, Department of Homeland Security*, GAO-03-102 (Washington, D.C.: Jan. 24, 2003).

## Balancing Homeland Security with Other National Budget Needs

The strategy notes that "the national effort to enhance homeland security will yield tremendous benefits and entail substantial financial and other costs." In April 2002 and September 2003, we reported that, among other things, the federal government must address the challenge of formulating realistic budget and resource plans that support and will sustain implementation of an efficient and effective homeland security program and that provide sufficient guidance to federal, state, local and private sector entities to create concurrent and compatible strategic plans and investments.[2] In this regard, extensive resources that have already been designated for homeland security, along with those resources currently being proposed, clearly reflect a large and rapidly growing federal role involving direct spending and assistance to others. While a robust homeland security program is critical to the nation's protection and prosperity, the challenge will be to develop it in a manner that is targeted to areas of greatest need and avoids wasteful, unfocused, or "hitchhiker" spending. Moreover, the new commitments will compete with and increase the pressure on other important priorities within the budget. As our long-term budget simulation notes, known demographic trends and rising health care costs will place unprecedented pressures on our long-range fiscal position. A fundamental review of existing programs and operations can create much-needed fiscal flexibility by weeding out programs that are outdated, poorly targeted, or inefficiently designed and managed. An additional challenge with regard to balancing homeland security funding with other national requirements involves the role of both the executive and legislative branches of government in ensuring optimum performance and appropriate accountability of our homeland security activities and program expenditures. The 9/11 Commission made recommendations related to this challenge.

## Providing Timely and Transparent Budget Information

The strategy reflects that "it is important to reprioritize spending to meet our homeland security needs, and not simply to permit unchecked overall growth in federal outlays." To examine homeland security as a crosscutting governmentwide function, Section 889 of the Homeland Security Act of 2002 requires that the President's budget include a funding analysis covering all federal homeland security activities—not just those

[2]See GAO, *Homeland Security: Responsibility and Accountability for Achieving National Goals*, *Statement of David M. Walker*, *Comptroller General of the United States*, GAO-02-627T (Washington, D.C.: Apr. 11, 2002); and *Truth and Transparency: The Federal Government's Financial Condition and Fiscal Outlook* (Washington, D.C.: Sept. 17, 2003).

carried out in DHS. As we reported in November 2002,[3] agencies provide information that distinguishes funding for homeland security from combating terrorism and other federal activities at a level of detail that OMB describes as sufficient to analyze government spending on homeland security. OMB has made a number of improvements to its annual *Report to Congress on Combating Terrorism*.[4] For the first time, the annual report issued in September 2003 aggregated funding information by the critical mission areas in the *National Strategy for Homeland Security*. Additionally, by releasing this year's analysis with the President's fiscal year 2005 budget, OMB has made this crosscutting presentation a timely complement to individual budget proposals and a resource for congressional budget deliberations. Despite these positive changes, congressional decision makers still face challenges in using this information to make sound decisions on appropriations. Specifically, a key element to understanding spending for homeland security is missing—that is, how much of the funding provided has been obligated. Without obligation information, it is impossible to know (1) whether funds are being used to implement programs (e.g., orders placed, contracts awarded, and services received); (2) how much funding from prior years is still available to potentially offset new needs or priorities; (3) whether the rate of spending for a program is slower than anticipated; or (4) what the level of effort or commitment is in a particular mission area for a given year or over time.

## Improving Risk Management Methods for Resource Allocation and Investment

The strategy states that "we must carefully weigh the benefit of each homeland security endeavor and only allocate resources where the benefit of reducing risk is worth the amount of additional cost." We have long advocated a risk management approach to guide the allocation of resources and investments for improving homeland security.[5] Additionally,

[3]GAO, *Combating Terrorism: Funding Data Reported to Congress Should Be Improved*, GAO-03-170 (Washington, D.C.: November 26, 2002).

[4]Consistent with the requirements of Fiscal Year 1998 National Defense Authorization Act, the annual *Report to Congress on Combating Terrorism* details governmentwide spending to combat terrorism. Starting with the fiscal year 2005 President's budget, in compliance with the Homeland Security Act of 2002, this information will be transmitted with the President's buget.

[5]See GAO, *Homeland Security: Key Elements of a Risk Management Approach*, GAO-02-150T (Washington, D.C.: Oct. 12, 2001); and *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: Oct. 31, 2001).

OMB has identified various tools it considers useful in planning, such as benefit-cost analysis, capital budgeting, and regulatory decision making.[6] Such tools are difficult to apply to homeland security expenditures even when such application is encouraged in the homeland security strategy.[7] A challenge to the central management of the budget is to develop and adopt a framework and supporting tools to inform cost allocations in a risk management process. Although OMB asked the public in 2002 for suggestions on how to adjust standard tools to the homeland security setting,[8] a vacuum currently exists in which benefits of homeland security investments are often not quantified and are almost never valued in monetary terms.[9] As OMB guidance is relatively silent on acceptable treatments of nonquantifiable benefits,[10] there is a lack of criteria to guide agency analysts in developing information to inform management. The Gilmore and 9/11 commissions made recommendations on the need for risk management.

## Establishing Baseline Performance Goals and Measures

While the strategy discusses creating benchmarks and performance measures, it does not provide a baseline set of performance goals and measures upon which to assess and improve preparedness. The Government Performance and Results Act of 1993 (GPRA) required federal agencies to develop strategic plans with long-term, outcome-oriented goals and objectives, annual goals linked to achieving the long-term goals, and annual reports on the results achieved. In July 2002,[11] we testified that because of lack of performance goals and measures in the homeland security strategy, the nation does not have a comprehensive set of performance goals and measures upon which to assess and improve prevention efforts, vulnerability reduction, and responsiveness to damage and recovery needs at all levels of government. Thus the nation faces a challenge to establish clear goals and performance measures to ensure

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

[7]OMB, Office of Information and Regulatory Affairs, *Informing Regulatory Decisions: 2003 Report to Congress on the Costs and Benefits of Federal Regulations and Unfunded Mandates on State, Local, and Tribal Entities* (Washington, D.C.: Sept. 2003).

[8]OMB, *2003 Report to Congress on Combating Terrorism* (Washington, D.C.: Sept. 2003).

[9]OMB Circular A-11.

[10]OMB Circular A-94.

[11]See GAO, *Homeland Security: Critical Design and Implementation Issues*, GAO-02-957T (Washington, D.C.: July 17, 2002).

both a successful and a fiscally responsible preparedness effort. We identified strategic planning as one of the critical success factors for new organizations. For example, as part of its implementation phase, we noted that DHS should engage in strategic planning through the involvement of stakeholders, assessment of internal and external environments, and an alignment of activities, core processes, and resources to support mission-related outcomes. We are currently reviewing DHS's first strategic plan to, among other things, assess the extent to which it reflects GPRA requirements and supports the strategy. The 9/11 Commission made recommendations related to this challenge.

## Clarifying Government and Private Sector Roles and Responsibilities

According to the strategy, "the responsibility for providing homeland security is shared between federal, state and local governments, and the private sector." In April 2002,[12] we testified, however, that the appropriate roles and responsibilities within and between the levels of governments and with the private sector are evolving and need to be clarified. New threats are prompting a reassessment and shifting of long-standing roles and responsibilities. These shifts have been occurring on a piecemeal and ad hoc basis without the benefit of an overarching framework and criteria to guide the process. The homeland security strategy recognizes the challenge posed by a complex structure of overlapping federal, state, and local governments—our country has more than 87,000 jurisdictions—but its initiatives often do not provide a baseline set of performance goals and measures upon which to assess and improve preparedness. Thus, the nation does not yet have a comprehensive set of performance goals and measures upon which to assess and improve prevention efforts, vulnerability reduction, and responsiveness to damage and recovery needs at all levels of government. Given the need for a highly integrated approach to the homeland security challenge, national performance goals and measures for strategy initiatives that involve both federal and nonfederal actors may best be developed in a collaborative way involving all levels of government and the private sector. Standards are one tool the homeland security strategy emphasizes in areas such as training, equipment, and communications. The 9/11 Commission made recommendations related to this challenge.

[12]See GAO, *Homeland Security: Responsibility and Accountability for Achieving National Goals*, GAO-02-627T (Washington, D.C.: Apr. 11, 2002).

## Developing a National Enterprise Architecture for Homeland Security

The strategy points out that mobilizing and organizing the nation to secure it from terrorist attacks is "an exceedingly complex mission that requires coordinated and focused effort from our entire society." The development of a national enterprise architecture could assist in transforming the various organizations involved in homeland security, as well as their supporting systems, in a way that eliminates duplication, promotes interoperability, reduces costs, and optimizes mission performance. An enterprise architecture is a blueprint that defines, both in logical terms (including interrelated business processes and business rules, integrated functions, applications, systems, users, work locations, and information needs and flows) and in technical terms (including hardware, software, data, communications, and security) how an organization operates today, how it will operate in the future, and a road map for the transition.

DHS intends to incrementally develop a national enterprise architecture for homeland security. In August 2004,[13] we reported that DHS's initial enterprise architecture provided a partial basis upon which to build future versions that can be made applicable beyond the department itself. However, it was missing most of the content necessary to be considered a well-defined architecture. Moreover, the content in this 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, along with their respective portfolios of system investment projects. Such a development approach is not consistent with recognized architecture development best practices. DHS officials agreed with our content assessment of their initial architecture, stating that it is largely a reflection of what could be done without a departmental strategic plan to drive architectural content and with limited resources and time. Since our report was published, DHS has developed the next version or increment of its enterprise architecture, with the intent of developing future versions or increments that extend horizontally to include, for example, state and local government homeland security entities. The 9/11 Commission made recommendations related to this challenge.

[13]See GAO, *Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains*, GAO-04-777 (Washington, D.C.: Aug. 6, 2004).

## Improving Governmentwide Information Technology Management

The strategy states that "every government official performing every homeland security mission depends upon information and information technology." However, in January 2004,[14] we reported that challenges are faced throughout the federal government with regard to information technology management—including the consistent application of IT strategic planning and performance measurement practices. Specifically, we have found that agencies generally have IT strategic plans and goals, but that these goals are not always linked to specific performance measures that are tracked. Additionally, while agencies largely have IT investment management boards, we found no agency had the practices associated with control fully in place. These practices are important ingredients for ensuring effective strategic planning and investment management, and they, in turn, make it more likely that the billions of dollars in government IT investments will be wisely spent. Finally, our experience with federal agencies has shown that attempts to modernize IT environments without blueprints—models simplifying the complexities of how agencies operate today, how they will operate in the future, and how they will get there—often result in unconstrained investment and systems that are duplicative and ineffective. Enterprise architectures, as described in our report, offer such blueprints. The 9/11 Commission made recommendations related to this challenge.

[14] See GAO, *Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved*, GAO-04-49 (Washington, D.C.: Jan. 12, 2004).

# Appendix IX: Department Summary Across Critical Mission Areas

This appendix provides a summary analysis across all the six mission areas. It includes information on whether all 43 initiatives are being covered, how frequently departments are cited with lead responsibilities, whether they are implementing programs related to these initiatives in fiscal year 2004, and where such implementation efforts are concentrated. As stated earlier, we used the *National Strategy for Homeland Security* and Homeland Security Presidential Directives 1 through 12 to determine lead agencies with respect to each initiative. The "clear" and "implied" leads, discussed in the methodology section, are denoted by solid and dashed line boxes, respectively.

**Table 13: Summary of Department Leads, Planning, and Implementation across the Six Critical Mission Areas of the National Strategy for Homeland Security**

| | DHS | | | DOJ | | | DOD | | | HHS | | | State | | | DOE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 |
| **1. Intelligence and warning** | | | | | | | | | | | | | | | | | | |
| (1) Enhance analytic capabilities of the FBI | | | | ● | ● | ● | | | | | | | | | | ● | | ● |
| (2) Build new capabilities through the Information Analysis and Infrastructure Protection Division of the proposed DHS | ● | ● | | | | | | | ● | | | | | | | ● | | ● |
| (3) Implement the Homeland Security Advisory System | ● | ● | | | | | | | ● | | | | | | | ● | | ● |
| (4) Utilize dual-use analysis to prevent attacks | ● | ● | | | | | | | | | | | ● | ● | ● | | ● | |
| (5) Employ "red-team" techniques | ● | ● | | | | | ● | | ● | | | | | | | | | ● |
| **2. Border and transportation Security** | | | | | | | | | | | | | | | | | | |
| (1) Ensure accountability in border and transportation security | ● | ● | ● | | | | ● | ● | ● | | ● | ● | ● | ● | ● | ● | | |
| (2) Create "smart borders" | ● | ● | ● | ● | ● | | | | | | ● | ● | ● | ● | ● | | | |
| (3) Increase the security of international shipping containers | ● | ● | ● | | | | ● | | ● | | | | ● | ● | ● | ● | | ● |
| (4) Implement the Aviation and Transportation Security Act of 2001 | | ● | ● | | | | | ● | ● | | | | | | | | | |
| (5) Recapitalize the U.S. Coast Guard | ● | ● | ● | | | | ● | ● | | | | | | | | | | |
| (6) Reform immigration services | ● | ● | ● | ● | ● | | | | | | | | ● | ● | ● | | | |
| **3. Domestic counterterrorism** | | | | | | | | | | | | | | | | | | |
| (1) Improve intergovernmental law enforcement coordination | | ● | ● | ● | ● | ● | ● | ● | ● | | ● | ● | | | | ● | | ● |
| (2) Facilitate apprehension of potential terrorists | ● | ● | ● | ● | ● | ● | | | ● | | | | ● | ● | ● | | | |
| (3) Continue ongoing investigations and prosecutions | ● | ● | ● | ● | ● | ● | | | | | | | | | | | | |
| (4) Complete FBI restructuring to emphasize prevention of terrorist attacks | | | | ● | ● | ● | | | | | | | | | | | | |
| (5) Target and attack terrorist financing | | ● | ● | ● | ● | ● | | | | | | | ● | ● | ● | | | |
| (6) Track foreign terrorists and bring them to justice | ● | ● | ● | ● | ● | ● | ● | ● | ● | | | | ● | ● | ● | ● | | ● |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Department IMPLICITLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

PI = Prior implementation to fiscal year 2004
RP = Recent planning
04 = Fiscal year 2004 implementation

Source: GAO.

*Continued on next page*

| | DHS | | | DOJ | | | DOD | | | HHS | | | State | | | DOE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 |
| **4. Protecting critical infrastructures and key assets** | | | | | | | | | | | | | | | | | | |
| (1) Unify America's infrastructure protection effort in DHS | ● | ● | | ● | | | ● | ● | ● | | ● | ● | | | | ● | | ● |
| (2) Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets | ● | ● | ● | ● | | | | ● | ● | ● | ● | ● | | | | ● | | ● |
| (3) Enable effective partnership with state and local governments and the private sector | | ● | ● | ● | ● | ● | | ● | | | ● | ● | | | | ● | | ● |
| (4) Develop a national infrastructure protection plan | | ● | ● | | | | | ● | | | ● | | | | | ● | ● | ● |
| (5) Secure cyberspace | | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | | ● | ● |
| (6) Harness the best analytic and modeling tools to develop effective protective solutions | | ● | ● | | | | | ● | ● | | ● | ● | | | | ● | | ● |
| (7) Guard America's critical infrastructure and key assets against "inside" threats | ● | ● | ● | | | | ● | ● | | | ● | ● | ● | ● | ● | ● | ● | ● |
| (8) Partner with the international community to protect our transnational infrastructure | | ● | ● | ● | ● | ● | ● | ● | ● | | ● | ● | ● | ● | ● | | | |
| **5. Defending against catastrophic threats** | | | | | | | | | | | | | | | | | | |
| (1) Prevent terrorist use of nuclear weapons through better sensors and procedures | ● | ● | ● | | | | ● | ● | ● | | | | ● | ● | ● | ● | ● | ● |
| (2) Detect chemical and biological materials and attacks | | ● | ● | | | | ● | ● | | ● | ● | ● | | | | ● | ● | ● |
| (3) Improve chemical sensors and decontamination techniques | | ● | ● | | | | | | | ● | ● | ● | | | | ● | ● | ● |
| (4) Develop broad spectrum vaccines, antimicrobials, and antidotes | | ● | ● | | | | | | | | ● | ● | ● | ● | ● | ● | | ● |
| (5) Harness the scientific knowledge and tools to counter terrorism | ● | ● | ● | | | | ● | | | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| (6) Implement the Select Agent Program | | | | | | | ● | | | ● | ● | ● | | | | | | |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Department IMPLICITLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

PI = Prior implementation to fiscal year 2004
RP = Recent planning
04 = Fiscal year 2004 implementation

Source: GAO.

*Continued on next page*

| | DHS | | | DOJ | | | DOD | | | HHS | | | State | | | DOE | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 | PI | RP | 04 |
| **6. Emergency preparedness and response** | | | | | | | | | | | | | | | | | | |
| (1) Integrate separate federal response plans into a single all-discipline incident management plan | | ● | ● | | | | | ● | ● | | ● | ● | | | | | ● | ● |
| (2) Create a national incident management system | | ● | ● | | | | | ● | | | ● | ● | | | | | ● | ● |
| (3) Improve tactical counter terrorist capabilities | ● | ● | ● | | | | | ● | | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| (4) Enable seamless communication among all responders | | ● | ● | | | | | | | ● | ● | ● | | | | | | |
| (5) Prepare health care providers for catastrophic terrorism | | ● | ● | | | | | ● | ● | ● | ● | ● | | | | | ● | ● |
| (6) Augment America's pharmaceutical and vaccine stockpiles | | ● | ● | | | | | ● | | ● | ● | ● | | | | | ● | ● |
| (7) Prepare for chemical, biological, radiological, and nuclear decontamination | | ● | ● | | | | ● | | ● | | ● | ● | | | | | ● | ● |
| (8) Plan for military support to civil authorities | | | ● | | | | ● | ● | ● | | | | | | | | | |
| (9) Build the Citizen Corps | | ● | ● | | | ● | | | | | | | | | | | | |
| (10) Implement the first responder initiative of the fiscal year 2003 budget | ● | | ● | ● | ● | ● | | | | | | | | | | | | |
| (11) Build a national training and evaluation system | | ● | ● | ● | | | | ● | | | ● | ● | | | | | | |
| (12) Enhance the victim support system | | ● | ● | | | ● | | | | | ● | ● | | | | | | |

● Indicates the department has planning and/or implementation activity related to this initiative

Department CLEARLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

Department IMPLICITLY identified as lead agency based on our review of Homeland Security Strategy and HSPDs

PI = Prior implementation to fiscal year 2004
RP = Recent planning
04 = Fiscal year 2004 implementation

Source: GAO.

The strategy identifies 43 initiatives across the six mission areas. All 43 initiatives have been addressed through department planning or implementation activities. Each initiative has been addressed by at least two departments under review, with a single exception (Justice is the only department involved in planning/implementing activities to complete the FBI's restructuring process to emphasize the prevention of terrorist attacks). A total of 33 initiatives have been addressed by three or more departments under review; 9 initiatives have been addressed by five or more departments.

All initiatives have identified leads, with one exception (the Intelligence and Warning initiative, "employment of red-team techniques"). The strategy and HSPDs intended DHS to be the prominent department on matters related to homeland security. This is reflected in DHS being identified as a lead on 37 of the 43 initiatives, spanning all six critical mission areas. DOJ is identified as a lead department on 8 of the 43 initiatives, including all 6 initiatives cited under the Domestic Counterterrorism mission area—the mission area most specifically related to criminal justice matters. (DOJ had been identified as a lead agency with respect to two initiatives, creating smart borders and guarding America's critical infrastructure and key assets against inside threats. However, given the transfer of the Immigration and Naturalization Service and the National Infrastructure Protection Center programs to the Department of Homeland Security, DOJ officials indicated the department no longer serves as a lead on these 2 initiatives). HHS is identified as a lead on 6 of the 43 initiatives. (HHS has no lead responsibilities with respect to the Intelligence and Warning, Border and Transportation Security, and Domestic Counterterrorism mission areas.) State is cited as a lead on 4 initiatives, spanning all the critical mission areas with the exception of Intelligence and Warning and Emergency Preparedness and Response. DOD has been cited in the homeland security strategy and HSPDs as a lead on 3 initiatives (excluding the Intelligence and Warning, Border and Transportation Security, and Domestic Counterterrorism mission areas). DOE is a lead department on 2 initiatives, encompassing just two critical mission areas: Protecting Critical Infrastructures and Key Assets and Defending against Catastrophic Threats.

The six departments under review have implemented activities on several initiatives during fiscal year 2004, for which they have been identified as leads. DHS cited implementation activities in 36 of the 37 initiatives for which it was identified as a lead (the one exception being the Select Agent Program). HHS, DOD, DOE, DOJ, and State cited implementation activities in fiscal year 2004 on each of their lead areas. In total, one or more departments cited implementation activities in fiscal year 2004 on all 43 initiatives.

When considering departmental implementation activities during fiscal year 2004, irrespective of lead, we find that DHS documented activities in 40 of the 43 initiatives, spanning all six critical mission areas. DOE documented fiscal year 2004 implementation activities in 25 of the 43 initiatives, also spanning all six critical mission areas. HHS identified 2004 activities in 24 of the 43 initiatives, covering five of the six mission areas (the exception: Intelligence and Warning). DOD cited 2004 implementation

activities in 17 of the 43 initiatives, covering all six mission areas. State demonstrated 2004 activities in 15 of the 43 initiatives, spanning all six mission areas; and DOJ identified 2004 activities in 13 of the 43 initiatives, covering four of the six mission areas (the exceptions: Border and Transportation Security and Defending against Catastrophic Threats).

# Appendix X: Homeland Security Presidential Directives

This appendix describes, in chronological order, the presidential directives that, in conjunction with the *National Strategy for Homeland Security* and certain other national strategies, form the foundation for the federal government's efforts to protect the nation against terrorist attack and ensure the security of the homeland. These documents set forth agencies' roles and responsibilities for responding to potential or actual terrorist threats or incidents as well as the processes and mechanisms by which the federal government mobilizes and deploys resources and coordinates assistance to state and local authorities, the public, and the private sector.

## Homeland Security Presidential Directive-1

HSPD-1 was issued on October 29, 2001. It established the Homeland Security Council (HSC) and charged it with ensuring that all homeland security-related activities carried out by the executive agencies and departments are properly coordinated and with promoting the effective development and implementation of all homeland security policies. In addition to describing the organization and operation of the HSC, it set forth the composition and duties of the HSC Principals Committee (the senior interagency forum under the HSC for homeland security issues) and the HSC Deputies Committee (the senior sub-Cabinet interagency forum for consideration of policy issues affecting homeland security). It also discussed the formation of the 11 HSC Policy Coordination Committees to serve as the main day-to-day forum for interagency coordination of homeland security policy.

## Homeland Security Presidential Directive-2

HSPD-2, also issued on October 29, 2001, set forth U.S. national policy for combating terrorism through the application of enhanced immigration policies designed to aggressively prevent the entry into the country of aliens who engage in or support terrorist activity and to identify, locate, detain, prosecute, and deport any such aliens already residing in the United States. This directive established the Foreign Terrorist Tracking Task Force to ensure federal agency coordination and directed the (1) development and implementation of multiyear plans to enhance the investigative and intelligence analysis capabilities of the INS and Customs Service; (2) implementation of measures to end the abuse of student visas and prohibit certain international students from receiving education and training in sensitive areas; (3) initiation of negotiations with Canada and Mexico to ensure maximum possible compatibility of immigration, customs, and visa policies; and (4) study of the use of advanced technologies for data sharing and enforcement efforts.

## Homeland Security Presidential Directive-3

Issued on March 11, 2002, HSPD-3 established the Homeland Security Advisory System (HSAS) as a comprehensive and effective means for ensuring the rapid dissemination of information regarding the risk of terrorist acts to federal, state, and local authorities and to the general public. It describes the HSAS as a system that provides warnings in the form of a set of graduated threat levels that increase as the risk of an attack rises and goes on to explain that for each threat level there would be a corresponding set of protective measures that would be implemented. According to HSPD-3, the HSAS is intended to create a common vocabulary, context, and structure for an ongoing national dialogue about the nature of the terrorist threat and the actions that can be taken in response to it.

## Homeland Security Presidential Directive-4

Issued in December 2002, HSPD-4 is the unclassified version of the *National Strategy to Combat Weapons of Mass Destruction*. This directive promulgates the nation's resolve to combat weapons of mass destruction through the application of new technologies, increased emphasis on intelligence collection and analysis, the strengthening of alliance relationships, and the establishment of new partnerships with former adversaries. Further, HSPD-4 sets forth the three principal pillars upon which the strategy will rest—counterproliferation to combat WMD use; strengthened nonproliferation to combat WMD proliferation; and consequence management to respond to WMD use. The classified version of this HSPD is NSPD-17.

## Homeland Security Presidential Directive-5

HSPD-5, issued on February 28, 2003, is concerned with the management of domestic terrorist attacks, major disasters, and other emergency incidents. It calls for the establishment of a single, comprehensive national incident management system in order to ensure that all levels of government across the nation have the capability to work together efficiently and effectively, using a national approach to domestic incident management. HSPD-5 further states that with regard to domestic incidents, the federal government will treat crisis management and consequence management as a single, integrated function, rather than as two separate functions. HSPD-5 is considered to be a companion to HSPD-8, which was issued in December 2003.

## Homeland Security Presidential Directive-6

Issued on September 16, 2003, HSPD-6 set forth the policy of the United States with regard to the integration and use of screening information. It directed the Attorney General to establish an organization to consolidate

the government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. HSPD-6 further directed that the heads of executive departments and agencies provide—to the extent permitted by law—the Terrorist Threat Integration Center with all appropriate terrorist information in their possession, custody, or control on an ongoing basis.

## Homeland Security Presidential Directive-7

HSPD-7 was issued on December 17, 2003, and established a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. It set forth the roles and responsibilities of the Secretary of Homeland Security, sector-specific federal agencies, and other departments, agencies, and offices in critical infrastructure protection. It should be noted that HSPD-7 superseded an earlier presidential directive on critical infrastructure protection (PDD 63).

## Homeland Security Presidential Directive-8

This directive was also issued on December 17, 2003. It established policies to strengthen the nation's preparedness to prevent and respond to potential or actual terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of federal preparedness assistance to state and local governments, and outlining actions to strengthen the preparedness capabilities of federal, state, and local entities. HSPD-8 is a companion to HSPD-5, which had been issued earlier in the year.

## Homeland Security Presidential Directive-9

HSPD-9, issued on January 30, 2004, established a national policy to defend the agriculture and food system of the United States against terrorist attacks, major disasters, and other emergencies. It set forth the roles and responsibilities of the Secretaries of Homeland Security, Agriculture, and Health and Human Services and the Administrator of the Environmental Protection Agency in ensuring the safety and security of the nation's food supply.

## Homeland Security Presidential Directive-10

HSPD-10 was issued on April 28, 2004, under the title "Biodefense for the 21st Century." It set forth a blueprint—based on a comprehensive evaluation of the nation's biological defense capabilities—for the nation's future biodefense program that fully integrates the sustained efforts of the national and homeland security, medical, public health, intelligence,

diplomatic, and law enforcement communities. HSPD-10 describes the pillars of the national biodefense program as threat awareness, prevention and protection, surveillance and detection, and response and recovery. Finally, it provided that specific direction to departments and agencies for implementing the biodefense program is contained in a classified version of the HSPD, NSPD-33.

## Homeland Security Presidential Directive-11

Issued on August 27, 2004, HSPD-11 builds on HSPD-6 in setting forth the nation's policy with regard to comprehensive terrorist-related screening procedures. Specifically, it states that terrorist-related screening will be enhanced through (1) the adoption of comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities that pose a threat to homeland security and (2) the implementation of a comprehensive and coordinated approach to terrorist-related screening—in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure—that supports homeland security.

## Homeland Security Presidential Directive-12

HSPD-12, also issued on August 27, 2004, directs the establishment of a common identification standard for federal employees and contractors. Specifically, HSPD-12 states that the policy of the United States is to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy through the establishment of a mandatory, governmentwide standard for secure and reliable forms of identification issued by the federal government.

# Appendix XI: Comments from the Department of Defense

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

ASSISTANT SECRETARY OF DEFENSE
2600 DEFENSE PENTAGON
WASHINGTON, DC 20301-2600

HOMELAND DEFENSE

24 NOV 2004

Mr. Norman J. Rabkin, Managing Director
Homeland Security and Justice Issues
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Rabkin:

We appreciate the opportunity to comment on the draft report, "HOMELAND SECURITY: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security." The Department of Defense applauds the efforts of the GAO to ensure that initiatives outlined in the *National Strategy for Homeland Security* are being addressed. As your report indicates, the Department of Defense is actively pursuing a diverse range of CIP security initiatives.

The Department would like to clarify one point with respect to the draft report. In Appendix V, DoD is identified as a lead agency for the initiative to "Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets." More accurately, it should be noted that DoD is the sector-specific lead for the Defense Industrial Base, while the Department of Homeland Security is charged with the overall lead for the initiative. Although Appendix V addresses this issue briefly, this distinction between overall lead and sector-specific lead is not self-evident in the report.

Let me take this opportunity to thank you and your staff for producing a thorough and accurate report.

Sincerely,

Paul McHale

## GAO Comment

We incorporated the point indicated in the DOD letter and responded to technical comments where appropriate throughout the report.

# Appendix XII: Comments From the Department of Health and Human Services

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Office of the Assistant Secretary for Public Health Emergency Preparedness
Washington, D.C. 20201

DEC - 6 04

Mr. Norman J. Rabkin, Managing Director
Homeland Security and Justice Issues
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Mr. Rabkin:

Thank you for this opportunity to comment on your draft report entitled: "Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security (GAO-05-33)." The enclosed comments and technical edits represent our department's understanding of the issues described.

We highlight the following issues for your attention, decontamination responsibilities and the transfer of the Strategic National Stockpile from Department of Homeland Security (DHS) back to HHS.

Once again, we appreciate the opportunity to contribute to this report.

Sincerely,

William F. Raub

William F. Raub
Deputy Principal Assistant Secretary
Office for Public Health Emergency Preparedness

Enclosure

**Comments of the Department of Health and Human Services to the General Accountability Office's Draft Report, "Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security." (GAO-05-33)**

General Comments and Technical Edits

The Department of Health and Human Services (HHS) appreciates the opportunity to comment on the Government Accountability Office's (GAO) draft report.

We offer the following general comments and technical edits:

1. Letter Report, Page 17 – HHS is listed as "implicitly identified" as lead agency for improving decontamination techniques based on GAO's review of the National Strategy for Homeland Security and Homeland Security Presidential Directives (HSPDs). We note two other provisions that cause some confusion regarding decontamination.

   First, in Appendix VII, Page 4 of your report (Item 7 in Table VII.1), you note that the Department of Homeland Security (DHS) is "clearly" identified as the lead for the task "Prepare for chemical, biological, radiological, and nuclear decontamination."

   Second, HSPD 10 suggests, at least implicitly, that the Environmental Protection Agency has the lead for decontamination in a biological incident:
   "The Administrator of the Environmental Protection Agency, in coordination with the Attorney General and the Secretaries of Defense, Agriculture, Labor, Health and Human Services, and Homeland Security, is developing specific standards, protocols, and capabilities to address the risks of contamination following a biological weapons attack and developing strategies, guidelines, and plans for decontamination of persons, equipment, and facilities."

   Finally, the HHS initiative mentioned in Appendix VI, Page 5 relates to chemical sensors (e.g., the Rapid Toxic Screen testing), not decontamination. Separating this item into two (chemical sensors and decontamination) would provide clarity.

2. Appendix II, Page 5 – HHS is listed as operating the BioWatch program. This is inaccurate. DHS manages this program with support from HHS. Please revise accordingly.

3. Appendix III, Page 5, 2nd line – "HHS' Food and Drug Service Administration..." should read "The Food and Drug Administration within HHS."

4. Appendix V, Page 4, 3rd line from bottom – "HHS' Food and Drug Service Administration..." should read "The Food and Drug Administration within HHS."

5. Appendix V, Page 4, 2nd and 3rd lines from bottom – For clarity, FDA issued five security guidance documents for different segments of the food industry which suggested conducting background checks. The FDA guidance was not directed at how to conduct the background checks, and was not directed only to the food service industry. Suggested re-phrasing is: "The Food and Drug Administration within HHS issued guidance to the food industry that suggested preventative measures, including employee background checks, which could increase the security of food while under an establishment's control."

6. Appendix V, Page 4, Table 4 – A dot should be included in item 2, "Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets", under the HHS PI column. FDA completed its initial vulnerability assessments of the food industry in 2002, while continuing to re-evaluate its assessments.

7. Appendix V, Page 4, top paragraph, 2nd line from bottom - Insert "food" after "agriculture", thus the phrase would read "addressing the terrorist threat to agriculture and food."

8. Appendix VII, Page 2 – The Project Bioshield 2004 legislation, signed by the President on July 21, 2004, returned the Strategic National Stockpile to HHS from DHS. In addition to the Stockpile, HHS maintains additional emergency preparedness and response assets, which include (but are not limited to) teams from the United States Public Health Service Commissioned Corps, the Centers for Disease Control and Prevention, and the Food and Drug Administration. Please revise accordingly.

9. Appendix VII, Page 10 – The Report notes that "DHS…will help hospitals 'expand their surge capacity to care for large numbers of patients in a mass-casualty incident.'" HSPD-10 notes that HHS "in coordination with other appropriate Federal departments and agencies, is the principal Federal agency responsible for coordinating all Federal-level assets activated to support and augment the state and local medical and public health response to mass casualty events." Please note this designation and revise accordingly.

10. Appendix IX, Page 2, Table 4 – A dot should be included in item 2, "Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets", under the HHS PI column. FDA completed its initial vulnerability assessments of the food industry in 2002, while continuing to re-evaluate its assessments.

## GAO Comment

We incorporated the technical comments where appropriate throughout the report.

# Appendix XIII: Comments From the Department of Homeland Security

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

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

Homeland Security

December 9, 2004

Mr. Norman Rabkin
Managing Director, Homeland Security & Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Rabkin:

RE: GAO-05-33, Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security (GAO Job Code 440295)

Thank you for the opportunity to review the subject draft report. It acknowledges the work and progress of the Department of Homeland Security (DHS) and the Departments of Justice, Defense, Health and Human Services, State and Energy in addressing the Administration's National Strategy for Homeland Security initiatives and the Homeland Security Presidential Directives (HSPDs) objectives through strategic planning and related activities in Fiscal Year 2004. DHS has a prominent role in implementing all six of the critical mission areas that include Border and Transportation Security, Domestic Counterterrorism, Protecting Critical Infrastructure and Key Assets, and Emergency Preparedness and Response.

We generally agree with the tenor of the report. Challenges remain in implementing the strategy in a well coordinated and integrated manner particularly when issues cut across two or more of the six critical mission areas. However, the report notes that all the national strategy's 43 initiatives are included in the activities of at least one of the six departments reviewed. DHS itself had planning and/or implementation activity related to 40 of the 43 initiatives. DHS and the other departments are individually and collectively moving forward to accomplish our respective missions with regard to implementing the National Strategy for Homeland Security.

The report identifies a baseline from which to assess progress in meeting homeland security objectives. It does not contain any recommendations. The Department Summary Across Critical Mission Areas (Appendix IX) and related table entitled Summary of Department Leads, Planning, and Implementation Across the Six Critical Mission Areas of the National Strategy for Homeland Security is particularly useful.

www.dhs.gov

We have enclosed information that reflects in part the on-going work of DHS in meeting many of the challenges facing America. In addition, we are assuming GAO's incorporation of our technical comments which were provided to your office under separate cover.

Sincerely,

Anna F. Dixon
Director
Departmental GAO/OIG Liaison Office

Enclosure

MMcP

**Enclosure**

Appendix II-Intelligence and Warning

Under "Challenge: Enhancing the analytical capabilities of the FBI" (page 7), we believe that the stand up of the US CERT gives DHS, and consequently the FBI through the law enforcement section, a better situational awareness of what is occurring across cyberspace and, in particular, in the government space. The later would be a natural target for terrorists.

In addition, DHS' support/administration of the Cybercop Portal serves as vehicle for sharing information (not classified, but important to the recipient) with our state and local partners within the cyber law enforcement community. Furthermore, DHS has acted as a conduit between the intelligence community/law enforcement and the private sector wherein source information has been rendered anonymous. DHS component(s) also have acted as another mechanism for passing cyber information from law enforcement to the intelligence community.

Appendix IV- Domestic Counterterrorism

While not specifically directed toward terrorism, the National Cyber Response Coordination Group (NCRCG) and the Cybercop Portal can be used toward that end.

Appendix V- Protecting Critical Infrastructures and Key Assets

One of the major initiatives in the critical infrastructure protection mission area is securing cyberspace. We believe that GAO should include or otherwise reference the NCRCG that is mentioned in the National Response Plan's Cyber Annex as a coordinating body for cyber emergencies of national scope.

Page 2, paragraph 1 discusses DHS primary responsibilities and provides examples of specific functions performed by DHS. GAO may want to include additional responsibilities mentioned in HSPD-7. This includes responsibility for chemicals, dams, and nuclear reactors, materials and waste.

Please consider including information related to Sector-Specific Agencies under Challenges in Critical Infrastructure Protection (Appendix V, pp. 7-16). HSPD-7 required the development of the National Infrastructure Protection Plan (NIPP). HSPD-7 recognizes that infrastructure sectors possess unique characteristics and operating models, and assigns Critical Infrastructure Protection (CIP) responsibilities for those sectors to Sector-Specific Agencies (SSAs), with guidance to be provided by DHS. To implement HSPD-7, SSAs have developed Sector-Specific Plans (SSPs) that provide an informational foundation for the NIPP. SSPs provide a detailed description of the specific processes that are used to identify, assess, prioritize, protect, and measure effectiveness; the plans for implementing these processes; and the status of any efforts being conducted to support this effort to date, including best practices identified, challenges encountered, and products generated. Additionally, these SSPs address many of the challenges documented in this section of Appendix V.

GAO notes three challenges related to federal CIP efforts on page 8. Progress meeting the challenges mentioned is imminent. The NIPP is on schedule to be approved this month as planned; the support to the Executive Order 13356 Working Group is developing information sharing relationships; the Interagency Incident Management Group has improved and the fusion cell will further strengthen DHS' ability to analyze threat, incident, and vulnerability information together in a meaningful way.

On page 14 of Appendix V, Challenge: Addressing chemical plant security, GAO, referring to a March 2003 report, states that the "federal government has not comprehensively assessed the industry's vulnerability to terrorist attacks" and, "as a result, federal, state, and local entities are challenged by a lack of comprehensive information on vulnerabilities faced by the sector." DHS through it Information Analysis and Infrastructure Protection Directorate has published several *Characteristics and Common Vulnerabilities* (CCV) and *Potential Indicators of Terrorist Activity* (PI) reports for the chemical sector, the latest revisions have been prepared in October 2004. Specific reports address chemical facilities, chemical storage, and chemical transportation.

Appendix V, Pages 14-15, Challenge: Addressing nuclear power plant security discusses problems reported by GAO in September 2003 with respect to the Nuclear Regulatory Commission (NRC)'s oversight of security at commercial nuclear power plants. GAO should note that an inter-agency (NRC, FBI and the DHS' United States Coast Guard and Emergency Preparedness and Response) team is developing plans to conduct comprehensive vulnerability assessments of commercial nuclear reactors and associated facilities. Each facility will be assessed and protective strategies prepared and implemented.

Appendix VI-Defending against Catastrophic Threats

Reference again should be made to the NCRCG. There has been speculation that a cyber attack would be used in conjunction with a physical attack to enhance the amount of damage. The NCRCG is activated in the event of a significant event (cyber or physical effecting cyber), and would be a coordinating body for response and reconstitution efforts.

Appendix VIII-Crosscutting Issues

Appendix VIII, Page 3, Challenge: Improving risk management methods for resource allocation and investment comments on the benefits of the risk management approach. DHS is working on a high-level risk-based approach to CIP. This effort is based in part on the methodology described in past GAO reports.

## GAO Comment

In addition to making the changes indicated in the enclosure, we incorporated the technical comments where appropriate throughout the report.

# Appendix XIV: Comments From the Department of Justice

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

U.S. Department of Justice

*Washington, D.C. 20530*

December 3, 2004

Norman J. Rabkin
Managing Director, Homeland Security and Justice
Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

RE: GAO Draft Audit Report No. GAO-05-33 (Review No. 440295)

Dear Mr. Rabkin:

The Department of Justice (Department) reviewed the final draft of the Government Accountability Office's (GAO) report entitled HOMELAND SECURITY: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security (GAO-05-33). The Department sent its technical comments, under separate cover to Jared Hermalin, the Analyst-in-Charge at GAO. Below find the Department's formal comments for inclusion in the final report that GAO publishes.

**APPENDIX IV**
**DOMESTIC COUNTERTERRORISM**

**Page 2, Agencies with Major Roles in Domestic Counterterrorism**
The first paragraph incorrectly says that the FBI leads the Anti-Terrorism Advisory Councils. In fact, the Executive Office of the United States Attorneys holds that responsibility. The FBI leads the Joint Terrorism Task Forces. In addition, the FBI has responsibility for terrorist financing which was left out of the paragraph completely. Consequently, we suggest the paragraph should read:

"*Of the six departments under review, the Departments of Justice (DOJ) and Homeland Security (DHS) have major roles in Domestic Counterterrorism. DOJ leads Anti-Terrorism Advisory Councils to increase cooperation between federal, state and local law enforcement. Within DOJ, the Federal Bureau of Investigation (FBI) works to detect and prevent terrorist acts through analysis and fieldwork to identify terrorists, their supporters, and materials that may be used to perpetrate a terrorist act, to include terrorist financing; tracks foreign terrorists and keeps them from entering the U.S.; and leads the multi-agency Joint Terrorism Task Forces (JTTFs). The Department's 94 United States Attorneys lead the Anti-Terrorism Advisory Councils that enhance cooperation and information sharing among federal, state and local law enforcement, first responders, industry, academia, and others.*"

The enclosed Statement of Recent Accomplishments describes some of the efforts to prevent terrorism taken since the GAO stopped collecting data for this report. Specifically, the Statement supplements the GAO report by detailing how the FBI realigned its assets and shifted its priorities to make the prevention of terrorism the Bureau's main priority. The GAO told the Department on October 24, 2004, to provide this data along with the Department's formal comments, and that the material would be included in the GAO final report.

The Department appreciates the opportunity to provide its formal comments and supplemental information. For more information, your staff may contact Richard Theis, Acting Director, Audit Liaison Office, on 202-514-0469.

Sincerely,

Paul R. Corts
Assistant Attorney General
for Administration

cc:
EOUSA - David L. Smith
FBI - Cheryl Johnston
JMD - Walt Wondolowski
Criminal - Julie Wellman
OJP - LeToya Johnson
ODAG - James A. McAtamney

Enclosure

**Statement of Recent Accomplishments**

Under the leadership of Director Mueller, the FBI has moved forward aggressively to implement a comprehensive plan that has fundamentally transformed the FBI with one goal in mind: establishing the prevention of terrorism as the Bureau's number one priority. While the FBI once concentrated on investigating terrorist crimes after they occurred; the FBI now focuses on disrupting terrorists before they strike. Director Mueller has overhauled the FBI's counterterrorism operations, expanded its intelligence capabilities, modernized its business practices and technology, and improved coordination with its partners.

To implement these new priorities, the FBI increased the number of Special Agents assigned to terrorism matters and hired additional intelligence analysts and translators. Also, it established operational units and entities that provide new or improved capabilities to address the terrorist threat. These include the 24/7 Counterterrorism Watch (CT Watch) and the National Joint Terrorism Task Force (NJTTF) to manage and share threat information; the Terrorism Financing Operation Section (TFOS) to centralize efforts to stop terrorist financing; document/media exploitation squads to exploit material found both domestically and overseas for its intelligence value; deployable "Fly Teams" to lend counterterrorism expertise wherever it is needed; the Terrorist Screening Center (TSC) and Foreign Terrorist Tracking Task Force (FTTTF) to help identify terrorists and keep them out of the United States; the Terrorism Reports and Requirements Section to disseminate FBI terrorism-related intelligence to the Intelligence Community; and the Counterterrorism Analysis Section to merge, compare, and assess indicators of terrorist activity against the United States from a strategic perspective.

The FBI centralized management of its Counterterrorism Program at Headquarters to limit "stove-piping" of information, to ensure consistency of counterterrorism priorities and strategies across the organization, to integrate counterterrorism operations here and overseas, to improve coordination with other agencies and governments, and to make senior FBI managers accountable for the overall development and success of its counterterrorism efforts.

The FBI is building an enterprise-wide intelligence program that has already improved substantially its ability to strategically direct its intelligence collection and to fuse, analyze, and disseminate its terrorism-related intelligence. The FBI quickly implemented a plan to integrate all its capabilities and better prevent terrorist attacks after passage of the USA PATRIOT Act, issuance of related Attorney General Guidelines, and an issuance of opinion by the Foreign Intelligence Surveillance Court of Review that removed the barrier to sharing information between intelligence and criminal investigations. Director Mueller elevated intelligence to program-level status, putting in place a formal structure and concepts of operations to govern FBI-wide intelligence functions, and establishing Field Intelligence Groups (FIGs) in every Bureau field office.

Understanding that the Bureau cannot defeat terrorism without strong partnerships, the FBI has enhanced the level of coordination and information sharing with state and municipal law enforcement personnel. The Bureau expanded the number of Joint Terrorism Task Forces (JTTFs), increased technological connectivity with its partners, and implemented new ways of sharing information through vehicles such as the FBI Intelligence Bulletin, the Alert System, and the Terrorist Screening Center. To improve coordination with other federal agencies and members of the Intelligence Community, the Bureau joined with its federal partners and established the Terrorist Threat Integration Center, exchanged personnel, instituted joint briefings, and started using secure networks to share information. The Bureau improved its relationships with foreign governments by building on the overseas expansion begun under Director Louis Freeh; by offering investigative and forensic support and training, and by working together with those governments on task forces and joint operations. Finally, the FBI expanded outreach to minority communities, and improved coordination with private businesses involved in critical infrastructure and finance.

Re-engineering its personnel efforts made the Bureau more efficient and more responsive to operational needs. The Bureau revised its approach to strategic planning, and refocused its recruiting and hiring to attract individuals with the skills critical to counterterrorism and intelligence missions. Also, the FBI developed a more comprehensive training program and instituted new leadership initiatives to keep its workforce flexible.

These improvements have produced tangible, measurable results. Since September 11, 2001, the FBI participated in disrupting dozens of terrorist operations by developing actionable intelligence and better coordinating our counterterrorism efforts. The Bureau significantly increased the number of human sources and the amount of surveillance coverage to support its counterterrorism efforts. It developed and refined a process for briefing daily threat information, and considerably increased the number of FBI intelligence reports produced and disseminated.

Prior to September 11, 2001, the Bureau had no centralized structure for the national management of its Counterterrorism Program, and terrorism cases were routinely managed out of individual field offices. An al-Qa'ida case, for example, might have been from the New York Field Office; a HAMAS case might have been managed by the Washington Field Office. This arrangement functioned for years, and produced a number of impressive prosecutions. Once counterterrorism became the overriding priority, improving the arrangement offered further benefits.

In December 2001, the Director reorganized and expanded the Counterterrorism Division (CTD) and created the position of Executive Assistant Director (EAD) for Counterterrorism and Counterintelligence. (The Assistant Director of CTD reports to the EAD.) The change centralized management, a predicate for a truly national program – to coordinate counterterrorism operations and intelligence production domestically and overseas; to conduct liaison with other agencies and governments; and to establish clear lines of accountability for the overall development and success of the FBI's Counterterrorism Program. With this management

structure in place, the FBI can affect a fundamental change in operations and can better accomplish its counterterrorism mission.

The FBI divided the operations of the Counterterrorism Division into branches, sections, and units, each of which focuses on a different aspect of the current terrorism threat facing the U.S. These components are staffed with intelligence analysts and subject matter experts who work closely with investigators in the field and integrate intelligence across component lines. This integration allows for real-time responses to threat information and quick communication with decision-makers and investigators in the field.

The FBI is designed, and has always operated, as both a law enforcement and intelligence agency. It has the dual mission: 1) to investigate and arrest perpetrators of completed crimes and 2) to collect intelligence that will help prevent future crimes and assist policy makers in their decision making. History has shown that the Bureau is most effective in protecting the United States (U.S.) when it performs these missions in tandem.

The FBI has long recognized that investigations produce intelligence benefits beyond arrest and prosecution. Starting with the Ku Klux Klan cases in the 1960's and the Mafia cases of the 1970's, FBI agents began to view criminal investigations as both a means of arresting and prosecuting someone for a completed crime, and as a means of obtaining information to prevent future crime. The goal was not simply to arrest individual members of the Klan or the Mafia, but to penetrate and dismantle a whole criminal organization.

As this approach was adopted, the FBI developed intelligence tools that have proven critical to predicting and preventing criminal activity. Also, the Bureau learned to think strategically before making arrests, sometimes opting to delay a suspect's arrest to allow more opportunity for surveillance that might disclose conspirators or other criminal plans. This approach was used to great effect in organized crime cases and espionage investigations, and members of the Bureau's Safe Streets Task Forces use it to combat street gangs. This is the approach that, since 9/11, the Bureau has used successfully in terrorism investigations.

By definition, investigations of international terrorism are both "intelligence" and "criminal" investigations. They are intelligence investigations because their objective, pursuant to Executive Order 12333, is "the detection and countering of international terrorist activities," and because they employ authorities and investigative tools – such as Foreign Intelligence Surveillance Act warrants – designed for the intelligence mission of protecting the U.S. against attack or other harm by foreign entities. They are criminal investigations because international terrorism against the U.S. constitutes a violation of the federal criminal code.

Over the past two decades, court rulings and internal DOJ procedures regarding FISA warrents barred FBI agents and other Intelligence Community personnel working intelligence cases from coordinating and swapping leads with agents working criminal cases. As a result of this legal "wall," intelligence agents and criminal agents working on a single terrorist target had to proceed independently and without knowing what the other may have been doing.

The USA PATRIOT Act, enacted on October 26, 2001 eliminated this "wall" and authorized coordination among agents working criminal matters and those working intelligence investigations. On March 6, 2002 the Attorney General issued new Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI (Intelligence Sharing Procedures) to capitalize on this legislative change. The new procedures specifically authorized agents working intelligence cases to disseminate to criminal prosecutors and investigators all relevant foreign intelligence information, including information obtained from FISA, in accordance with applicable minimization standards and other specific restrictions. Likewise, the procedures authorized prosecutors and criminal agents to advise FBI agents working intelligence cases on all aspects of foreign intelligence investigations, including the use of FISA.

On November 18, 2002 the Foreign Intelligence Surveillance Court of Review issued an opinion approving the Intelligence Sharing Procedures. The opinion authorized the FBI to share information, including FISA-derived information, with both criminal and intelligence investigators. Today, the FBI can conduct terrorism investigations using criminal and intelligence tools and personnel.

To FBI formalized this merger of intelligence and criminal operations by abandoning its practice of classifying cases as either "criminal" or "intelligence" international terrorism investigations; now the FBI classifies all these cases as ones including "international terrorism." This reclassification officially designates an international terrorism investigation as one that can employ intelligence tools as well as criminal processes and procedures. In July 2003, the Bureau formalized this approach in its Model Counterterrorism Investigative Strategy (MCIS), which was issued to all field offices and has been the subject of extensive field training.

With the dismantling of the legal "wall" and the integration of criminal and intelligence personnel and operations, the FBI now has the latitude to coordinate its intelligence and criminal investigations and to employ full range of investigative tools against a suspected terrorist. On the intelligence side, it can conduct surveillance on the suspected terrorist to learn about his movements and identify possible confederates; it can obtain FISA authority to monitor his conversations; and/or it can approach and attempt to cultivate him as a source or an operational asset. On the criminal side, the Bureau has the option of incapacitating him through arrest, detention, and prosecution. The course to take is chosen by continuously balancing the opportunity to develop intelligence against the need to apprehend the suspect and prevent him from carrying out his terrorist plans. This integrated approach has guided Bureau operations and enabled it foil terrorist-related operations and disrupt cells from Northern Virginia, to Buffalo, New York, to Portland, Oregon, to Newark, New Jersey.

**Virginia Jihad Network**

As a result of an FBI, Washington Field Office investigation, nine members of a group based in Northern Virginia, now known as the Virginia Jihad Network, were convicted on charges to include: Conspiracy to levy war against the United States (18 USC 2384); Conspiracy to provide material support to Al-Qa'ida (18 USC 2339B); Conspiracy to provide material support to Lashkar-e-Taiba (18 USC 2339A); and supplying services to the Taliban (50 US 1705.)

The investigation, which involved both intelligence and criminal aspects, proved that members of the Virginia Jihad Network had intentionally participated in activities in preparation to enter into jihad (Holy War) against enemies of Islam, including the U.S. Specifically, members of the group participated in weekly jihad training sessions consisting of physical training in small-unit para-military tactics using paint-ball as a means of instruction, as well as religious instruction on the topics of jihad, typically through the readings of certain hadiths related to jihad.

**Lackawanna Six**

The FBI investigation known as the "Lackawanna Six," conducted by agents in the Buffalo Field Office, resulted in the convictions of six men, all U.S. citizens of Yemeni descent, for their participation in an Al-Qa'ida military-style training camp with radical Islamists in Afghanistan shortly before the 9/11 terrorist attacks. Five of the men plead guilty to providing material support to Al-Qa'ida and the sixth pled guilty to conducting transactions unlawfully with Al-Qa'ida.

The investigation successfully identified and documented the methods Al-Qa'ida members used to communicate with and recruit U.S. citizens of Yemeni descent to travel to Afghanistan for the purpose of military training for jihad.

**The Portland Seven**

The FBI, Portland Field Office, investigation known as the "Portland Seven," resulted in the conviction of seven Muslim men from Portland, in February 2004, for: Conspiracy to levy war against the United States; Conspiracy to Provide Material Support and Resources to Al-Qaida; Conspiracy to Contribute Services to Al-Qa'ida and the Taliban; and for two of the men: Possessing Firearms in Furtherance of Crimes of Violence.

The investigation proved that, as part of the conspiracy, members would travel to Afghanistan to join Al-Qa'ida and Taliban forces in the jihad and take up arms against the U.S. and allied military forces. Following the 9/11 terrorist attacks five of the defendants acquired various firearms and engaged in weapons training and physical training for preparation to fight a jihad. In October 2001, six of the men traveled to China, then tried several times to reach Afghanistan to fight for the Taliban.

**Hemant Lakhani**

The FBI investigation into the activities of businessman Hemant Lakhani, a British national born in India, resulted in charges against Lakhani for attempting to sell anti-aircraft missiles to shoot down American airliners. He was charged, also, with plotting to obtain for terrorists a "dirty bomb". Lakhani since pleaded not guilty to the charges of providing material support to terrorists and attempting to sell arms without a license. His trial is set to begin in November, 2004. If convicted, he could be sentenced to 25 years in prison.

Two other individuals were arrested and charged with helping in a planned money transfer that was part of the transaction. One of those two individuals arrived in the U.S. to allegedly arrange for a $500,000 down payment from a government cooperating witness for 50 more shoulder-fired missiles. Each individual faces up to five years in prison.

Although the FBI is now able to coordinate its intelligence collection and criminal law enforcement operations, it will realize its full potential as a terrorism prevention agency once it develops the intelligence structure, capabilities, and processes to direct those operations. The Department needs an effective intelligence capacity, if it expects to defeat a sophisticated and opportunistic adversary like Al-Qa'ida.

For a variety of historical reasons, the Bureau had not developed this intelligence capacity prior to September 11, 2001. Even though the FBI always has been one of the world's best collectors of information, it never completed the infrastructure to exploit that information fully for its intelligence value. Individual FBI agents analyzed the evidence in their particular cases, and used it to guide their investigations. The FBI as an institution, however, had not elevated that analytical process above the individual case or investigation to an overall effort to analyze intelligence and strategically direct intelligence collection against threats across all programs.

The attacks of September 11, 2001, highlighted, the need to develop an intelligence process for the Counterterrorism Program. Since then, the Bureau has undertaken to build the capacity to fuse, analyze, and disseminate its terrorism-related intelligence, and to direct investigative activities based on an analysis of gaps in its collection against national intelligence requirements. That effort has proceeded in four stages.

The first was to increase the number of analysts working counterterrorism. Immediately after September 11, Director Muller temporarily reassigned analysts from the Criminal Investigative and Counterintelligence Divisions to various units in the Counterterrorism Division. In July 2002, 25 analysts were detailed from the CIA to assist. Many of these analysts provided tactical intelligence analysis; others provided strategic "big picture" analysis. These deployments were temporary, but the progress made, the confidence gained, and the lessons learned during this period started the FBI down the road toward a functioning intelligence analysis operation. Also, the Bureau established the College of Analytical Studies to help train and develop a cadre of FBI specialized analysts.

On December 3, 2001, the Director established the Office of Intelligence (OI) within the Counterterrorism Division. The OI was responsible for establishing and executing standards for recruiting, hiring, training, and developing the intelligence analytic workforce, and ensuring that analysts are assigned to operational and field divisions based on intelligence priorities. Recognizing that intelligence and analysis are integral to all of the Bureau's programs, in February 2003, Director Mueller moved the OI out of the Counterterrorism Division and created a stand-alone OI, headed by an Executive Assistant Director (EAD-I), to provide centralized support and guidance for the Bureau's intelligence functions.

The second stage in the Bureau's intelligence integration was to elevate intelligence functions to program-level status, instituting centralized management and implementing a detailed blueprint for the Intelligence Program.

The Director articulated a clear mission for the Intelligence Program – to position the FBI to meet current and emerging national security and criminal threats by: 1) aiming investigative work proactively against threats; 2) building and sustaining enterprise-wide intelligence policies and capabilities; and 3) providing useful, appropriate, and timely information and analysis to the national security, homeland security, and law enforcement communities. With the mission defined, the Bureau set out to embed intelligence processes into the day-to-day work of the FBI, from the initiation of a preliminary investigation to the development of FBI-wide strategies.

Now that the Intelligence Program is established and evolving, the FBI is moving on to the third stage of transforming the Bureau into an intelligence agency – reformulating personnel and administrative procedures to instill within our workforce an expertise in the processes and objectives of intelligence work.

A major element of the Bureau's transformation is its increasing integration and coordination with its partners in the U.S. and international law enforcement and intelligence communities. More than any other type of enforcement mission, counterterrorism requires the participation of every level of local, state, national, and international government. A good example is the case of the Lackawanna terrorist cell outside Buffalo, New York. From the police officers who helped to identify and conduct surveillance on the cell members; to the CIA officers who provided information from their sources overseas; to the diplomatic personnel who coordinated our efforts with foreign governments; to the FBI agents and federal prosecutors who conducted the investigation leading to the arrests and indictments, everyone played a significant role.

The FBI recognizes that a prerequisite for any operational coordination is the full and free exchange of information. Without procedures and mechanisms that allow information sharing on a regular and timely basis, the Bureau and its partners cannot expect to align their operational efforts to best accomplish their common mission. Accordingly, the FBI took steps to establish FBI-wide policies for sharing information and intelligence.

To ensure a coordinated, enterprise-wide approach, the Director recently designated the EAD-I to serve as the principal FBI official for information and intelligence sharing policy. In this capacity, the EAD-I functions as an advisor to the Director and provides policy direction on information and intelligence sharing within and outside the FBI with the law enforcement and intelligence communities, as well as foreign governments. On February 20, 2004, the Bureau formed an information sharing policy group, comprised of Executive Assistant Directors, Assistant Directors and other senior executive managers. Under the Direction of the EAD-I, this group is establishing FBI information and intelligence sharing policies.

Beyond these information sharing initiatives, the Bureau is increasing its operational coordination with its state, federal, and international partners on a number of fronts.

The FBI strengthened its working relationships with the CIA and other members of the Intelligence Community. From the Director's daily meetings with the Director of Central Intelligence and CIA briefers, to the regular exchange of personnel among agencies, to the joint efforts in specific investigations and in the Terrorist Threat Integration Center, the Terrorist Screening Center, and other multiagency entities, the FBI and its partners in the Intelligence Community are now integrated at virtually every level of our operations.

The Terrorist Threat Integration Center (TTIC) is a good example of the collaborative relationship among the FBI, the CIA, and other federal partners. Established on May 1, 2003, at the direction of President Bush, TTIC coordinates strategic analysis of threats based on intelligence from the FBI, CIA, DHS, and DOD. Analysts from each agency work side-by-side in one location to piece together the big picture of threats to the U.S. and our interests. TTIC analysts synthesize government-wide information regarding current terrorist threats and produce the Presidential Terrorism Threat Report for the President. FBI personnel at TTIC are part of the Office of Intelligence and work closely with analysts at FBI Headquarters in combining domestic and international terrorism developments into a comprehensive analysis of terrorist threats. In addition to the analysis developed by FBI analysts detailed to TTIC, FBI analysts at Headquarters regularly contribute articles to the President's Terrorist Threat Report.

The FBI currently has agents and analysts detailed to CIA entities, including the CIA's Counterterrorism Center (CTC). Also, FBI agents and intelligence analysts are detailed to the NSA, the National Security Council, DIA, the Defense Logistics Agency, DOD's Regional Commands, the Department of Energy, and other federal and state agencies.

CIA personnel are also working in key positions throughout the Bureau. The Deputy Section Chief of the International Terrorism Operations Section in the Counterterrorism Division is a CIA detailee. CIA officers are detailed to the Security Division, including the Assistant Director, the Chief of the Personnel Security Section, and managers working with the Secret Compartmental Information (SCI) program and the FBI Police. An experienced manager from the CIA's Directorate of Science and Technology now heads the Investigative Technologies Division and a CIA employee on detail serves as the Chief of a Section.

This exchange of personnel is taking place in Bureau field offices as well as in the FBI headquarters. In JTTF sites, the CIA has officers co-located with FBI agents, and there are plans to add CIA officers at several others. The NSA detailed analysts to FBI Headquarters, and the Washington, New York, and Baltimore Field Offices.

The FBI now uses secure systems to disseminate classified intelligence reports and analytical products to the Intelligence Community and other federal agencies. Improving the compatibility of information technology systems throughout the Intelligence Community will increase the speed and ease of information sharing and collaboration. To that end, an FBI information technology team worked with the Chief Information Officers (CIOs) of DHS and other Intelligence Community agencies as the Bureau upgraded its data systems.

DHS plays a critical role in assessing and protecting vulnerabilities in our national infrastructure and at our borders, and in overseeing our response capabilities. The Bureau has worked closely with DHS to ensure that the integration of information sharing between the agencies. The FBI and DHS share database access at TTIC, in the National JTTF at FBI Headquarters, in the FTTTF and the TSC, and in local JTTFs around the country. The FBI and DHS worked together to establish the new Terrorist Screening Center. CTD analysts from the FBI weekly brief their DHS counterparts on terrorism developments. The agencies jointly produce Intelligence Bulletins for state, local, and tribal law enforcement and state and local homeland security officials. They produce joint threat assessments for key events such as the national political party conventions. The Bureau designated an experienced executive from the Transportation Security Administration to run the TSC and detailed a senior DHS executive to the FBI's Office of Intelligence to ensure coordination and transparency between the agencies.

On March 4, 2003, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence signed a comprehensive Memorandum of Understanding (MOU) establishing policies and procedures for information sharing, handling, and use. Pursuant to that MOU, information related to terrorist threats and vulnerabilities is provided to DHS automatically. Consistent with the protection of sensitive sources and methods and the protection of privacy rights, we now share as a rule, and withhold by exception.

With terrorists traveling, communicating, and planning attacks around the world, coordination with our foreign partners has become more critical than ever before. The FBI has increased its overseas presence and now routinely deploys agents and crime scene experts to assist in the investigation of overseas attacks, such as the May 2003 bombings in Saudi Arabia and Morocco. Their efforts, and the relationships that grew from them, have played a critical role in the successful international operations the Bureau conducted over the past three years.

Bureau personnel have participated in numerous investigations of terrorist attacks in foreign countries. The approach taken to those investigations differs from the traditional Bureau approach. Prior to September 11, FBI overseas investigations were primarily focused on building cases for prosecution in the U.S. Today, the focus has broadened. Now, the FBI provides its foreign partners with investigative, forensic, and other types of support that enhance joint efforts

to prevent and disrupt terrorist attacks. This approach won the approval of our partners and increased reciprocal cooperation and led to more effective joint investigations.

With the recent directives implementing the intelligence agent career track and the administrative reforms related to building an intelligence workforce, the FBI has created a foundation for an intelligence-driven counterterrorism operation.

The substantial progress achieved over the past three years, defies precise measurement. However, several accomplishments demonstrate the effectiveness of the Counterterrorism Program. Including:

- Developing human assets
- Increasing the number of FISAs
- Increasing the number of intelligence reports generated
- Increasing the quality of daily briefings
- Raising the effectiveness of counterterrorism operations

The FBI historically has recognized that human sources often provide the most important information during a criminal investigation. Accordingly, the Bureau has developed expertise in recruiting and using human sources. Further, it uses those skills to great effect across a wide range of investigative programs, including organized crime, drugs, public corruption, and white collar crime.

The Bureau has placed a priority on developing human intelligence sources to assist in the identification and apprehension of international terrorists. The Bureau has revised its training programs, its personnel evaluation criteria, and its operational priorities to focus on source development. These efforts already increased the number of human intelligence sources in the Counterterrorism Program. Between August 30, 2001, and September 30, 2003, the number of sources related to international terrorism increased by more than 60 percent, and the number of sources related to domestic terrorism increased by more than 39 percent.

FISA coverage increased significantly, reflecting both the Bureau's increased focus on counterterrorism and counterintelligence investigations and its improvement in FISA operations. From 2001 to 2003, the number of FISA applications filed annually with the Foreign Intelligence Surveillance Court increased by 85 percent. The FISA has seen a similar increase in the use of the emergency FISA process that permits the FBI to obtain immediate coverage in emergency situations. In 2002, for example, the Department of Justice obtained a total of 170 emergency FISA authorizations, which is more than three times the number of emergency FISAs obtained in the 23 years between the 1978 enactment of FISA and September 11, 2001.

The fourth stage involves improved dissemination of information. In the past year, the FBI produced more than 3,000 intelligence products, including "raw" reports, intelligence memoranda, in-depth strategic analysis assessments, special event threat assessments, and focused Presidential briefings. In addition, it briefed many members of Congress, other government agencies, and law enforcement organization about intelligence matters.

Prior to September 11, 2001, the FBI produced very few raw intelligence reports. In fiscal 2004, the FBI produced and disseminated about 2,700 Intelligence Information Reports (IIRs) containing raw intelligence derived from FBI investigations and intelligence collection. The majority contained intelligence related to international terrorism; the next greatest number contained foreign intelligence and counterintelligence information; and the remainder concerned criminal activities and cyber crime. These IIRs were sent to a wide customer set in FBI field offices, the Intelligence Community, Defense Community, other federal law enforcement agencies, and U.S. policy entities.

In addition to these raw intelligence reports, the FBI has begun producing analytic assessments on a par with those the Intelligence Community produces. The FBI developed and issued, in January 2003, a classified comprehensive assessment of the terrorist threat to the U.S. This assessment focuses on the threats that may develop over the next two years, based on an analysis of information regarding the motivations, objectives, methods, and capabilities of existing terrorist groups and the potential for the emergence of new terrorist groups. This threat assessment is used as a guide in the allocation of investigative resources, as a compilation of threat information for investigators and intelligence personnel within and without the FBI, and as a resource for decision-makers elsewhere in the government. The 2004 threat assessment was released in April 2004. Also, the Bureau published a comprehensive assessment of the terrorist WBRN threat to the U.S., in December 2003. FBI analysts have produced 137 in-depth analyses in Fiscal Year 2004 and several hundred current intelligence articles.

How the FBI used the Al-Qa'ida terrorism handbook provides a good example of the Bureau's improved capacity to exploit evidence for its intelligence value. A terrorism handbook seized from an Al-Qa'ida location overseas in the mid-1990's was declassified and released by DOJ shortly after the events of September 11, 2001. The FBI believed, and subsequent events confirmed, that intelligence gleaned from the handbook could provide useful guidance about Al-Qa'ida's interests and capabilities. Nine Intelligence Bulletins were based in whole or in part on this intelligence. In addition, the Bureau used information from the Al-Qa'ida Handbook to update the Bureau's counterterrorism training, including the Intelligence Analyst Basic Course at the College of Analytical Studies, the Introduction to Counterterrorism Course at the National Academy, and sessions on Terrorism Indicators and Officer Safety in the Bureau's SLATT training.

One measure of the Bureau's improved counterterrorism operations is the Bureau's capability to analyze data daily and deliver daily briefing. The development of this capability reflects the maturation of the centralized Counterterrorism Program.

Prior to September 11, the FBI lacked the capacity to provide a comprehensive daily terrorism briefing – to assemble the current threat information, to determine what steps were being taken to address each threat, and to present a clear picture of each threat and the Bureau's response to that threat to the Director, senior managers, the Attorney General, and others in the Administration who make operational and policy decisions. Because investigations were run by individual field offices, the Bureau never developed a central repository of treat data. During the past three years,

with the assistance of veterans from the Intelligence Community, the FBI has established the infrastructure and the cadre of professionals to produce effective daily briefings and to share briefing materials more widely within the Bureau and with our partners.

In 2002, the Bureau established the Presidential Support Group within the Counterterrorism Division to prepare daily briefing materials. In the summer of 2003, this group was renamed the Strategic Analysis Unit and moved to the Office of Intelligence. Beginning in August 2003, the Strategic Analysis Unit began producing the Director's Daily Report (DDR), a daily intelligence briefing that includes information on counterterrorism operations, terrorism threats, and information related to all areas of FBI investigative activity. The DDR is distributed to executives in all FBI operational divisions. The Director uses the DDR to brief the President nearly every weekday morning. The FBI also produces *Presidential Intelligence Assessments*, finished FBI intelligence products covering topics of particular interest to the President on issues other than terrorism.

Director Mueller holds threat briefings twice a day: an intelligence briefing in the morning and a case-oriented briefing later in the day. At them, a briefer and the operational executive managers provide a summary of current threats and associated FBI operations. Because CIA and DHS representatives attend, these meetings facilitate the sharing of threat information. The development of the Bureau's daily briefings provides a tangible measure of progress.

The Bureau historically measured its performance, to a large extent, by the number of criminals it arrested. Although useful for traditional law enforcement, a new standard was needed to measure how well the Bureau neutralized terrorist threats. The arrest standard failed to account for terrorist threats neutralized through means other than formal terrorism prosecutions – such as deportation, detention, arrest on non-terrorism charges, seizure of financial assets, and the sharing of information with foreign governments for their use in taking action against terrorists within their borders.

The number of disruptions and dismantlement provides a better measure. This measure counts every time the Bureau – either by itself or with its partners in the law enforcement and intelligence communities – conducts an operation which disables, prevents, or interrupts terrorist fund-raising, recruiting, training, or operational planning. Since September 11, 2001, the FBI has participated in dozens of such operations, disrupting a wide variety of domestic and international terrorist undertakings.

The FBI has made significant advances over the past three years, as the forgoing shows.

## GAO Comments

In addition to the letter reprinted in this appendix, we included the enclosure containing the recent accomplishments of the Federal Bureau of Investigation. We did not solicit this type of information from any participating department nor its components, during this engagement. Nor did we conduct the necessary audit to verify the validity of the findings. In addition to providing the letter and enclosure, the department provided technical comments. We incorporated the technical comments where appropriate throughout the report.

# Appendix XV: GAO Contacts and Staff Acknowledgments

## GAO Contacts

### Intelligence and Warning

FBI Law Enforcement Issues
Laurie E. Ekstrand, (202) 512-2758

FBI Information Technology and Watch List Issues
Randolph C. Hite, (202) 512-6256

DHS Homeland Security Advisory System Issues
William O. Jenkins, Jr., (202) 512-8757

Threat Information Sharing Issues
Henry L. Hinton, (202) 512-6599

### Border and Transportation Security

Border, Customs and Immigration Issue
Richard M. Stana, (202) 512-8816

Visa Issues
Jess T. Ford, (202) 512-4268

Travel Document Counterfeiting and Fraud
Robert J. Cramer, (202) 512-7227

Border Radiation Detection Issues
Eugene E. Aloise, (202) 512-6870

Biometrics Technology Issues
Keith A. Rhodes, (202) 512-3938

Border Information Technology Issues
David A. Powner, (202) 512-9286

Aviation Security Issues
Cathleen A. Berrick, (202) 512-3404

Surface Transportation Security Issues
Cathleen A. Berrick, (202) 512-3404

Maritime Security Issues
Margaret T. Wrightson, (415) 904-2200

U.S. Coast Guard Issues
Margaret T. Wrightson, (415) 904-2200

## Domestic Counterterrorism

FBI Law Enforcement Issues
Laurie E. Ekstrand, (202) 512-2758

Money Laundering Issues
Richard M. Stana, (202) 512-8816

International Terrorist Financing Issues
Loren Yager, (202) 512-4347

Identification Counterfeiting and Fraud
Robert J. Cramer, (202) 512-7227

Social Security Number Fraud Issues
Barbara D. Bovbjerg, (202) 512-5491

## Protecting Critical Infrastructures and Key Assets

National Critical Infrastructure Protection Issues
Robert F. Dacey, (202) 512-3317

Cybersecurity Issues
Robert F. Dacey, (202) 512-3317

Protecting Government Buildings
Mark L. Goldstein, (202) 512-6670

Federal Protective Service Issues
Mark L. Goldstein, (202) 512-6670

Defense Installation Protection Issues
Janet A. St. Laurent, (202) 512-4402

Financial Services Sector Security Issues
Thomas J. McCool, (202) 512-8678

Postal and Shipping Safety and Security Issues
Katherine A. Siggerud, (202) 512-6570

Nuclear Power and Weapons Security Issues
Robin M. Nazzaro, (202) 512-6246

Water Utilities Security Issues
Robin M. Nazzaro, (202) 512-6246

Agricultural Sector Security Issues
Larry Dykman, (202) 512-9692

Chemical Plants Security Issues
John B. Stephenson, (202) 512-6225

## Defending Against Catastrophic Threats

Nonproliferation Issues (Department of Energy)
Eugene E. Aloise, (202) 512-6870

Nonproliferation Issues (Department of State)
Joseph A. Christoff, (202) 512-8979

Sales of Potentially Harmful Excess DOD Materials
Robert J. Cramer, (202) 512-7227

Bioterrorism Preparedness Issues
Janet Heinrich, (202) 512-7250

Bioterrorism Information Technology Issues
David A. Powner, (202) 512-9286

Defense Role in Weapons of Mass Destruction
Sharon L. Pickup, (202) 512-9619

Research and Development Issues
Eugene E. Aloise, (202) 512-6870

## Emergency Preparedness and Response

First Responder Emergency Preparedness Issues
William O. Jenkins, (202) 512-8757

Public Health Preparedness Issues
Janet Heinrich, (202) 512-7250

Defense Support to Civilian Agencies
Davi M. D'Agostino, (202) 512-5431

## Crosscutting Issues

National Strategy Issues
Norman J. Rabkin, (202) 512-8777

Strategic Planning and Results Issues
Bernice Steinhardt, (202) 512-6534

Human Capital Management Issues
Christopher J. Mihm, (202) 512-3236

Budget Issues
Paul L. Posner, (202) 512-9573

Risk Management and Resource Allocation
Scott R. Farrow, (202) 512-6669

Information Technology Issues
Randolph C. Hite, (202) 512-6256

Acquisition Management
Katherine V. Schinasi, (202) 512-4841

## Staff Acknowledgments

The following persons made key contributions to this report: Stephen L. Caldwell, Jared A. Hermalin, Wayne A. Ekblad, and Ricardo A. Marquez. In addition, numerous other individuals across GAO made contributions regarding the challenges faced in implementing the *National Strategy for Homeland Security*.

# Related GAO Products

## Intelligence and Warning

*Intelligence Reform: Human Capital Considerations Critical to 9/11 Commission's Proposed Reforms*. GAO-04-1084T. Washington, D.C.: September 14, 2004.

*Information Technology: Foundational Steps Being Taken to Make Needed FBI Systems Modernization Management Improvements*. GAO-04-842. Washington, D.C.: September 10, 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.

*FBI Transformation: Human Capital Strategies May Assist the FBI in Its Commitment to Address Its Top Priorities*. GAO-04-817T. Washington, D.C.: June 3, 2004.

*Security Clearances: FBI Has Enhanced Its Process for State and Local Law Enforcement Officials*. GAO-04-596. Washington, D.C.: April 30, 2004.

*FBI Transformation: FBI Continues to Make Progress in Its Efforts to Transform and Address Priorities*. GAO-04-578T. Washington, D.C.: March 23, 2004.

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

*Homeland Security Advisory System: Preliminary Observations Regarding Threat Level Increases from Yellow to Orange*. GAO-04-453R. Washington, D.C.: February 26, 2004.

*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.

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

*Post-Hearing Questions from the May 8, 2003, Hearing on Barriers to Information Sharing at the Department of Homeland Security*. GAO-03-985R. Washington, D.C.: July 7, 2003.

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

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

*Combating Terrorism: Actions Needed to Improve Force Protection for DOD Deployment through Domestic Seaports*. GAO-03-15. Washington, D.C.: October 22, 2002

*Homeland Security: Information Sharing Activities Face Continued Management Challenges*. GAO-02-1122T. Washington, D.C.: September 23, 2002.

## Border and Transportation Security

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

*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.

*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.

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

*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.

*Social Security Numbers: Use Is Widespread and Protections Vary in Private and Public Sectors*. GAO-04-1099T. Washington, D.C.: September 28, 2004.

*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.

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

*Border Security: Additional Actions Needed to Eliminate Weaknesses in the Visa Revocation Process*. GAO-04-795. Washington, D.C.: July 13, 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: Performance of Information Systems to Monitor Foreign Students and Exchange Visitors Has Improved but Issues Remain*. GAO-04-690. Washington, D.C.: June 18, 2004.

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

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

*Aviation Security: Private Security Screening Contractors Have Little Flexibility to Implement Innovative Approaches*. GAO-04-505T. Washington, D.C.: April 22, 2004.

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

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

*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.

*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.

*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.

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

*Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*. GAO-04-385. Washington, D.C.: February 12, 2004.

*The Department of Homeland Security Needs to Fully Adopt a Knowledge-based Approach to Its Counter-MANPADS Development Program*. GAO-04-341R. Washington, D.C.: January 30, 2004.

*Department of Homeland Security, Bureau of Customs and Border Protection: Required Advance Electronic Presentation of Cargo Information*. GAO-04-319R. Washington, D.C.: December 18, 2003.

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

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

*Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs*. GAO-04-285T. Washington, D.C.: November 20, 2003.

*Aviation Security: Efforts to Measure Effectiveness and Address Challenges*. GAO-04-232T. Washington, D.C.: November 5, 2003.

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

*Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining*. GAO-03-1173. Washington, D.C.: September 24, 2003.

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

*Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain*. GAO-03-1155T. 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.

*Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*. GAO-03-770. Washington, D.C.: July 25, 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-03-798. Washington, D.C.: June 18, 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.

*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.

*Transportation Security: Federal Action Needed to Address Security Challenges*. GAO-03-843. Washington, D.C.: June 30, 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.

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

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

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

*Homeland Security: Challenges to Implementing the Immigration Interior Enforcement Strategy*. GAO-03-660T. Washington, D.C.: April 10, 2003.

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

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

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

*Weaknesses in Screening Entrants into the United States*. GAO-03-438T. Washington, D.C.: January 30, 2003.

*Aviation Safety: Undeclared Air Shipments of Dangerous Goods and DOT's Enforcement Approach*. GAO-03-22. Washington, D.C.: January 10, 2003.

*Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges*. GAO-03-263. Washington, D.C.: December 13, 2002.

*Border Security: Implications for Eliminating the Visa Waiver Program*. GAO-03-38. Washington, D.C.: November 22, 2002.

*Homeland Security: INS Cannot Locate Many Aliens because It Lacks Reliable Address Information*. GAO-03-188. Washington, D.C.: November 21, 2002.

*Technology Assessment: Using Biometrics for Border Security*. GAO-03-174. Washington, D.C.: November 15, 2002.

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

*Border Security: Visa Process Should Be Strengthened as an Antiterrorism Tool*. GAO-03-132NI. Washington, D.C.: October 21, 2002.

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

*Mass Transit: Challenges in Securing Transit Systems*. GAO-02-1075T. Washington, D.C.: September 18, 2002.

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

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

*Aviation Security: Vulnerabilities in, and Alternatives for, Preboard Screening Security Operations*. GAO-01-1171T. Washington, D.C.: September 25, 2001.

*Aviation Security: Weaknesses in Airport Security and Options for Assigning Screening Responsibilities*. GAO-01-1165T. Washington, D.C.: September 21, 2001.

*Aviation Security: Terrorist Acts Demonstrate Urgent Need to Improve Security at the Nation's Airports*. GAO-01-1162T. Washington, D.C.: September 20, 2001.

*Aviation Security: Terrorist Acts Illustrate Severe Weaknesses in Aviation Security*. GAO-01-1166T. Washington, D.C.: September 20, 2001.

## Domestic Counterterrorism

*FBI Transformation: Data Inconclusive on Effects of Shift to Counterterrorism-Related Priorities on Traditional Crime Enforcement.* GAO-04-1036. Washington, D.C.: August 31, 2004.

*Combating Terrorism: Federal Agencies Face Continuing Challenges in Addressing Terrorist Financing and Money Laundering*. GAO-04-501T. Washington, D.C.: March 4, 2004.

*Investigations of Terrorist Financing, Money Laundering, and Other Financial Crimes*. GAO-04-464R. Washington, D.C.: February 20, 2004.

*Terrorist Financing: U.S. Agencies Should Systematically Assess Terrorists' Use of Alternative Financing Mechanisms*. GAO-04-163. Washington, D.C.: November 14, 2003.

*Combating Money Laundering: Opportunities Exist to Improve the National Strategy*. GAO-03-813. Washington, D.C.: September 26, 2003.

*FBI Reorganization: Progress Made in Efforts to Transform, but Major Challenges Continue*. GAO-03-759T. Washington, D.C.: June 18, 2003.

*Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*. GAO-03-959. Washington, D.C.: September 25, 2003.

*FBI Reorganization: Initial Steps Encouraging, but Broad Transformation Needed*. GAO-02-865T. Washington, D.C.: June 21, 2002.

*Foreign Languages: Workforce Planning Could Help Address Staffing and Proficiency Shortfalls*. GAO-02-514T. Washington, D.C.: March 12, 2002.

*Foreign Languages: Human Capital Approach Needed to Correct Staffing and Proficiency Shortfalls*. GAO-02-375. Washington, D.C.: January 31, 2002.

*Homeland Security: Justice Department's Project to Interview Aliens after September 11, 2001*. GAO-03-459. Washington, D.C.: April 11, 2003.

## Critical Infrastructure Protection

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*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.

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

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

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

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

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

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

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

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

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

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

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

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

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

## Defending against Catastrophic Threats

*Nuclear Nonproliferation: DOE Needs to Consider Options to Accelerate the Return of Weapons-Usable Uranium from Other Countries to the United States and Russia*. GAO-05-57. Washington, D.C.: November 19, 2004.

*Nuclear Nonproliferation: DOE Needs to Take Action to Further Reduce the Use of Weapons-Usable Uranium in Civilian Nuclear Reactors*. GAO-04-807. Washington, D.C.: July 30, 2004.

*Department of State: Nonproliferation, Anti-terrorism, Demining, and Related Programs Follow Legal Authority, but Some Activities Need Reassessment*. GAO-04-521. Washington, D.C.: April 30, 2004.

*Nonproliferation: Improvements Needed for Controls on Exports of Cruise Missile and Unmanned Aerial Vehicle Technology*. GAO-04-493T. Washington, D.C.: March 9, 2004.

*Missile Defense: Actions Being Taken to Address Testing Recommendations, but Updated Assessment Needed*. GAO-04-254. Washington, D.C.: February 26, 2004.

*Weapons of Mass Destruction: Defense Threat Reduction Agency Addresses Broad Range of Threats, but Performance Reporting Can Be Improved*. GAO-04-330. Washington, D.C.: February 13, 2004.

*Nonproliferation: Strategy Needed to Strengthen Multilateral Export Control Regimes*. GAO-03-43. Washington, D.C.: October 25, 2002.

*Chemical and Biological Defense: DOD Should Clarify Expectations for Medical Readiness*. GAO-02-219T. Washington, D.C.: November 7, 2001.

*Chemical and Biological Defense: DOD Needs to Clarify Expectations in Medical Readiness*. GAO-02-38. Washington, D.C.: October 19, 2001.

*Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness*. GAO-02-162T. Washington, D.C.: October 17, 2001.

*Bioterrorism: Review of Public Health Preparedness Programs*. GAO-02-149T. Washington, D.C.: October 10, 2001.

*Bioterrorism: Public Health and Medical Preparedness*. GAO-02-141T. Washington, D.C.: October 9, 2001.

*Bioterrorism: Coordination and Preparedness*. GAO-02-129T. Washington, D.C.: October 5, 2001.

*Bioterrorism: Federal Research and Preparedness Activities*. GAO-01-915. Washington, D.C.: September 28, 2001.

## Emergency Preparedness and Response

*Effective Regional Coordination Can Enhance Emergency Preparedness*. GAO-04-1009. Washington, D.C.: September 15, 2004.

*Infectious Disease Preparedness: Federal Challenges in Responding to Influenza Outbreaks*. GAO-04-1100T. Washington, D.C.: September 28, 2004.

*Homeland Security: Federal Leadership Needed to Facilitate Interoperable Communications between First Responders*. GAO-04-1057T. Washington, D.C.: September 8, 2004.

*September 11: Health Effects in the Aftermath of the World Trade Center Attack*. GAO-04-1068T. Washington, D.C.: September 8, 2004.

*HHS's Efforts to Promote Health Information Technology and Legal Barriers to Its Adoption*. GAO-04-991R. Washington, D.C.: August 13, 2004.

*Health Care: National Strategy Needed to Accelerate the Implementation of Information Technology*. GAO-04-947T. Washington, D.C.: July 14, 2004.

*Homeland Security: Coordinated Planning and Standards Needed to Better Manage First Responder Grants in the National Capital Region*. GAO-04-904T. Washington, D.C.: June 24, 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.

*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.

*Emergency Preparedness: Federal Funds for First Responders*. GAO-04-788T. Washington, D.C.: May 13, 2004.

*National Emergency Grants: Labor Is Instituting Changes to Improve Award Process, but Further Actions Are Required to Expedite Grant Awards and Improve Data*. GAO-04-496. Washington, D.C.: April 16, 2004.

*Project SAFECOM: Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration*. GAO-04-494. Washington, D.C.: April 16, 2004.

*Public Health Preparedness: Response Capacity Improving, but Much Remains to Be Accomplished*. GAO-04-458T. Washington, D.C.: February 12, 2004.

*HHS Bioterrorism Preparedness Programs: States Reported Progress but Fell Short of Program Goals for 2002*. GAO-04-360R. Washington, D.C.: February 10, 2004.

*Smallpox Vaccination: Review of the Implementation of the Military Program*. GAO-04-215R. Washington, D.C.: December 1, 2003.

*Homeland Security: Challenges in Achieving Interoperable Communications for First Responders*. GAO-04-231T. Washington, D.C.: November 6, 2003.

*September 11: Overview of Federal Disaster Assistance to the New York City Area*. GAO-04-72. Washington, D.C.: October 31, 2003.

*U.S. Postal Service: Clear Communication with Employees Needed before Reopening the Brentwood Facility*. GAO-04-205T. Washington, D.C.: October 23, 2003.

*Bioterrorism: Public Health Response to Anthrax Incidents of 2001*. GAO-04-152. Washington, D.C.: October 15, 2003.

*Infectious Diseases: Gaps Remain in Surveillance Capabilities of State and Local Agencies*. GAO-03-1176T. Washington, D.C.: September 24, 2003.

*Homeland Security: Reforming Federal Grants to Better Meet Outstanding Needs*. GAO-03-1146T. Washington, D.C.: September 3, 2003.

*Hospital Preparedness: Most Urban Hospitals Have Emergency Plans but Lack Certain Capacities for Bioterrorism Response*. GAO-03-924. Washington, D.C.: August 6, 2003.

*Severe Acute Respiratory Syndrome: Established Infectious Disease Control Measures Helped Contain Spread, but a Large-Scale Resurgence May Pose Challenges*. GAO-03-1058T. Washington, D.C.: July 30, 2003.

*Homeland Defense: DOD Needs to Assess the Structure of U.S. Forces for Domestic Military Missions*. GAO-03-670. Washington, D.C.: July 11, 2003.

*U.S. Postal Service: Issues Associated with Anthrax Testing at the Wallingford Facility*. GAO-03-787T. Washington, D.C.: May 19, 2003.

*SARS Outbreak: Improvements to Public Health Capacity Are Needed for Responding to Bioterrorism and Emerging Infectious Diseases*. GAO-03-769T. Washington, D.C.: May 7, 2003.

*Smallpox Vaccination: Implementation of National Program Faces Challenges*. GAO-03-578. Washington, D.C.: April 30, 2003.

*Homeland Defense: Preliminary Observations on How Overseas and Domestic Missions Impact DOD Forces*. GAO-03-677T. Washington, D.C.: April 29, 2003.

*Infectious Disease Outbreaks: Bioterrorism Preparedness Efforts Have Improved Public Health Response Capacity, but Gaps Remain*. GAO-03-654T. Washington, D.C.: April 9, 2003.

*Bioterrorism: Preparedness Varied across State and Local Jurisdictions*. GAO-03-373. Washington, D.C.: April 7, 2003.

*Homeland Security: CDC's Oversight of the Select Agent Program*. GAO-03-315R. Washington, D.C.: November 22, 2002.

*Homeland Security: New Department Could Improve Coordination, but Transferring Control of Certain Public Health Programs Raises Concerns*. GAO-02-954T. Washington, D.C.: July 16, 2002.

*Homeland Security: New Department Could Improve Biomedical R&D Coordination but May Disrupt Dual-Purpose Efforts*. GAO-02-924T. Washington, D.C.: July 9, 2002.

*Homeland Security: New Department Could Improve Coordination but May Complicate Public Health Priority Setting*. GAO-02-883T. Washington, D.C.: June 25, 2002.

*Combating Terrorism: Intergovernmental Cooperation in the Development of a National Strategy to Enhance State and Local Preparedness*. GAO-02-550T. Washington, D.C.: April 2, 2002.

*Combating Terrorism: Enhancing Partnerships through a National Preparedness Strategy*. GAO-02-549T. Washington, D.C.: March 28, 2002.

*Combating Terrorism: Critical Components of a National Strategy to Enhance State and Local Preparedness*. GAO-02-548T. Washington, D.C.: March 25, 2002.

*Combating Terrorism: Intergovernmental Partnership in a National Strategy to Enhance State and Local Preparedness*. GAO-02-547T. Washington, D.C.: March 22, 2002.

*Combating Terrorism*: *Key Aspects of a National Strategy to Enhance State and Local Preparedness*. GAO-02-473T. Washington, D.C.: March 1, 2002.

*Bioterrorism: The Centers for Disease Control and Prevention's Role in Public Health Protection*. GAO-02-235T. Washington, D.C.: November 15, 2001.

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

*Anthrax Vaccine: Changes to the Manufacturing Process*. GAO-02-181T. Washington, D.C.: October 23, 2001.

*Homeland Security: Need to Consider VA's Role in Strengthening Federal Preparedness*. GAO-02-145T. Washington, D.C.: October 15, 2001.

## Crosscutting Issues

*Homeland Security: Further Action Needed to Promote Successful Use of Special DHS Acquisition Authority*. GAO-05-136. Washington, D.C.: December 15, 2004.

*Information Technology: Major Federal Networks That Support Homeland Security Functions*. GAO-04-375. Washington, D.C.: September 17, 2004.

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

*Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains*. GAO-04-777. Washington, D.C.: August 6, 2004.

*Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach*. GAO-04-702. Washington, D.C.: August 27, 2004.

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

*Human Capital: Building on the Current Momentum to Transform the Federal Government*. GAO-04-976T. Washington, D.C.: July 20, 2004.

*Financial Management: Department of Homeland Security Faces Significant Financial Management Challenges*. GAO-04-774. Washington, D.C.: July 19, 2004.

*Status of Key Recommendations GAO Has Made to DHS and Its Legacy Agencies*. GAO-04-865R. Washington, D.C.: July 2, 2004.

*Department of Homeland Security: Financial Management Challenges*. GAO-04-945T. Washington, D.C.: July 8, 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.

*Human Capital: DHS Faces Challenges in Implementing Its New Personnel System*. GAO-04-790. Washington, D.C.: June 18, 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.

*Additional Posthearing Questions Related to the Proposed Department of Homeland Security Human Capital Regulations*. GAO-04-617R. Washington, D.C.: April 30, 2004.

*Transfer of Budgetary Resources to the Department of Homeland Security*. GAO-04-329R. Washington, D.C.: April 30, 2004.

*Reserve Forces: Observations on Recent National Guard Use in Overseas and Homeland Missions and Future Challenges*. GAO-04-670T. Washington, D.C.: April 29, 2004.

*Human Capital: Opportunities to Improve Federal Continuity Planning Guidance*. GAO-04-384. Washington, D.C.: April 20, 2004.

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

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

*Department of Homeland Security: Challenges and Steps in Establishing Sound Financial Management*. GAO-03-1134T. Washington, D.C.: September 10, 2003.

*Combating Terrorism: Observations on National Strategies Related to Terrorism*. GAO-03-519T. Washington, D.C.: March 3, 2003.

*Major Management Challenges and Program Risks: A Governmentwide Perspective*. GAO-03-95. Washington, D.C.: January 1, 2003.

*Major Management Challenges and Program Risks: Department of Homeland Security*. GAO-03-102. Washington, D.C.: January 1, 2003.

*Major Management Challenges and Program Risks: Department of Justice*. GAO-03-105. Washington, D.C.: January 1, 2003.

*Major Management Challenges and Program Risks: Federal Emergency Management Agency*. GAO-03-113. Washington, D.C.: January 1, 2003.

*Combating Terrorism: Funding Data Reported to Congress Should Be Improved*. GAO-03-170. Washington, D.C.: November 26, 2002.

*Highlights of a GAO Forum on Mergers and Transformation: Lessons Learned for a Department of Homeland Security and Other Federal Agencies*. GAO-03-293SP. Washington, D.C.: November 14, 2002.

*Homeland Security: Management Challenges Facing Federal Leadership*. GAO-03-260. Washington, D.C.: December 20, 2002.

*Homeland Security: Effective Intergovernmental Coordination Is Key to Success*. GAO-02-1013T. Washington, D.C.: August 23, 2002.

*Homeland Security: Effective Intergovernmental Coordination Is Key to Success*. GAO-02-1012T. Washington, D.C.: August 22, 2002.

*Homeland Security: Effective Intergovernmental Coordination Is Key to Success*. GAO-02-1011T. Washington, D.C.: August 20, 2002.

*Homeland Security: Critical Design and Implementation Issues*. GAO-02-957T. Washington, D.C.: July 17, 2002.

*Homeland Security: Title III of the Homeland Security Act of 2002*. GAO-02-927T. Washington, D.C.: July 9, 2002.

*Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success*. GAO-02-901T. Washington, D.C.: July 3, 2002.

*Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success*. GAO-02-900T. Washington, D.C.: July 2, 2002.

*Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success*. GAO-02-899T. Washington, D.C.: July 1, 2002.

*Homeland Security: New Department Could Improve Coordination but May Complicate Priority Setting*. GAO-02-893T. Washington, D.C.: June 28, 2002.

*Homeland Security: Proposal for Cabinet Agency Has Merit, but Implementation Will be Pivotal to Success*. GAO-02-886T. Washington, D.C.: June 25, 2002.

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

*National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy*. GAO-02-811T. Washington, D.C.: June 7, 2002.

*Homeland Security: Responsibility and Accountability for Achieving National Goals*. GAO-02-627T. Washington, D.C.: April 11, 2002.

*National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security.* GAO-02-621T. Washington, D.C.: April 11, 2002.

*Homeland Security: Progress Made; More Direction and Partnership Sought.* GAO-02-490T. Washington, D.C.: March 12, 2002.

*Homeland Security: Challenges and Strategies in Addressing Short- and Long-Term National Needs.* GAO-02-160T. Washington, D.C.: November 7, 2001.

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

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

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

## 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