

January 2003

Major Management Challenges and Program Risks

Department of
Homeland Security



G A O

Accountability * Integrity * Reliability

A Glance at the Agency Covered in This Report

The Department of Homeland Security (DHS) was established on January 24, 2003. This new cabinet department's primary mission is to prevent terrorist attacks within the United States, reduce the vulnerability of the United States to terrorism, and minimize the damage and assist in the recovery from attacks that do occur. The new department combines 22 federal agencies specializing in various disciplines, such as law enforcement, border security, biological research, computer security, and disaster mitigation. With an anticipated budget of almost \$40 billion and an estimated 170,000 employees, DHS is expected to be the third largest government agency. DHS will be organized into four divisions:

- Border and Transportation Security;
- Emergency Preparedness and Response;
- Chemical, Biological, Radiological, and Nuclear Countermeasures; and
- Information Analysis and Infrastructure Protection.

The Coast Guard and Secret Service will report directly to the Secretary for Homeland Security. The new department also will be responsible for the non-homeland security functions of the agencies being merged into DHS, including the Customs Service's trade enforcement mission, the Coast Guard's marine safety responsibilities, and the Federal Emergency Management Agency's natural disaster recovery efforts.

This Series

This report is part of a special GAO series, first issued in 1999 and updated in 2001, entitled the *Performance and Accountability Series: Major Management Challenges and Program Risks*. The 2003 Performance and Accountability Series contains separate reports covering each cabinet department, most major independent agencies, and the U.S. Postal Service. The series also includes a governmentwide perspective on transforming the way the government does business in order to meet 21st century challenges and address long-term fiscal needs. The companion 2003 *High-Risk Series: An Update* identifies areas at high risk due to either their greater vulnerabilities to waste, fraud, abuse, and mismanagement or major challenges associated with their economy, efficiency, or effectiveness. A list of all of the reports in this series is included at the end of this report.

Department of Homeland Security



Highlights of [GAO-03-102](#), a report to Congress included as part of GAO's Performance and Accountability Series

Why GAO Did This Report

The new Department of Homeland Security (DHS) faces unique opportunities and risks for ensuring the nation's homeland security. The implementation and transformation of DHS will be complex, and the components being merged into the new department already face a wide array of existing challenges. The information GAO presents in this report is intended to sustain congressional attention and a departmental focus on addressing these challenges. This report is part of a special series of reports on governmentwide and agency-specific issues.

What Needs to Be Done

DHS must effectively integrate disparate agencies and activities into a cohesive organization to achieve the synergy for providing better homeland security against terrorism. DHS should adopt public and private sector best practices, and build necessary management capacity and oversight mechanisms to implement and transform the new department. DHS also must create and maintain a structure that can leverage partners and stakeholders to effectively implement the national homeland security strategy. Finally, DHS must confront a wide array of existing major management challenges and program risks in its incoming agencies.

www.gao.gov/cgi-bin/getrpt?GAO-03-102.

To view the full report, click on the link above. For more information, contact Randall Yim at (202) 512-3580 or yimr@gao.gov or Patricia Dalton at (202) 512-6806 or daltonp@gao.gov.

What GAO Found

DHS faces enormous challenges to protect the nation from terrorism. DHS must effectively combine 22 agencies with an estimated 170,000 employees specializing in various disciplines, including law enforcement, border security, biological research, computer security, and disaster mitigation. Further, DHS will oversee a number of non-homeland security activities.

GAO has designated the implementation and transformation of DHS as a high risk 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, components being merged into DHS already face a wide array of existing challenges that must be addressed. Finally, DHS's failure to effectively carry out its mission exposes the nation to potentially very serious consequences.

Building an effective department will require sustained leadership from top management to ensure the transformation of disparate agencies, programs, and missions into an integrated organization. DHS leadership can learn from the best practices of the private and public sectors to become a high-performance organization. Achieving the national homeland security strategy will require the current transition plan to be more comprehensive by addressing the full transition period and by identifying key activities and milestones. Critical aspects of DHS's success will depend on well-functioning relationships with third parties that will take time to establish and maintain, including those with states and local governments, the private sector, and other federal agencies with homeland security responsibilities. DHS's leadership will also need to focus on certain critical success factors, including human capital, information technology management, acquisition management, and financial management to create a results-oriented and accountable department for the long term.

The new department is being formed from components with a wide array of existing major management challenges and program risks. In fact, many of the major components merging into the new department, including the Immigration and Naturalization Service, the Transportation Security Administration, Customs Service, Federal Emergency Management Agency, and the Coast Guard, face at least one major problem such as strategic human capital risks, information technology management challenges, or financial management vulnerabilities; they also confront an array of program operations challenges and risks.

In the final analysis, the success of DHS's implementation and transformation will depend largely on its ability to attract and retain the right people; set the appropriate priorities for the department; and build effective partnerships with the appropriate public, private, and not-for-profit sector entities.

Contents

Transmittal Letter	1
Major Performance and Accountability Challenges	2
GAO Contacts	35
Related GAO Products	36
Performance and Accountability and High-Risk Series	51

This is a work of the U.S. Government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. It may contain copyrighted graphics, images or other materials. Permission from the copyright holder may be necessary should you wish to reproduce copyrighted materials separately from GAO's product.



United States General Accounting Office
Washington, D.C. 20548

January 2003

The President of the Senate
The Speaker of the House of Representatives

This report addresses the major management challenges and program risks facing the Department of Homeland Security (DHS) as it is formed through one of the largest, most complex mergers ever undertaken. The government has a unique opportunity to transform a disparate group of agencies into a strong and effective cabinet department.

The implementation and transformation of this new department is an enormous undertaking that comes with significant risk. GAO has designated the implementation and transformation of DHS as a high-risk area for three reasons. First, the size and complexity of the effort make the challenge especially daunting. Second, the components being merged into DHS already face a wide array of existing challenges that must be addressed. Finally, DHS's failure to effectively carry out its mission exposes the nation to potentially very serious consequences.

This report provides an overview of the new department's challenges and program risks as it seeks to simultaneously establish itself and protect the nation from terrorism. This analysis should help the new Congress and the administration carry out their responsibility and improve government for the benefit of the American people. For additional information about this report, please contact Randall Yim, Managing Director, National Preparedness Team at (202) 512-3580, or at yimr@gao.gov, or Patricia A. Dalton, Director, Strategic Issues, at (202) 512-6806, or at daltonp@gao.gov.

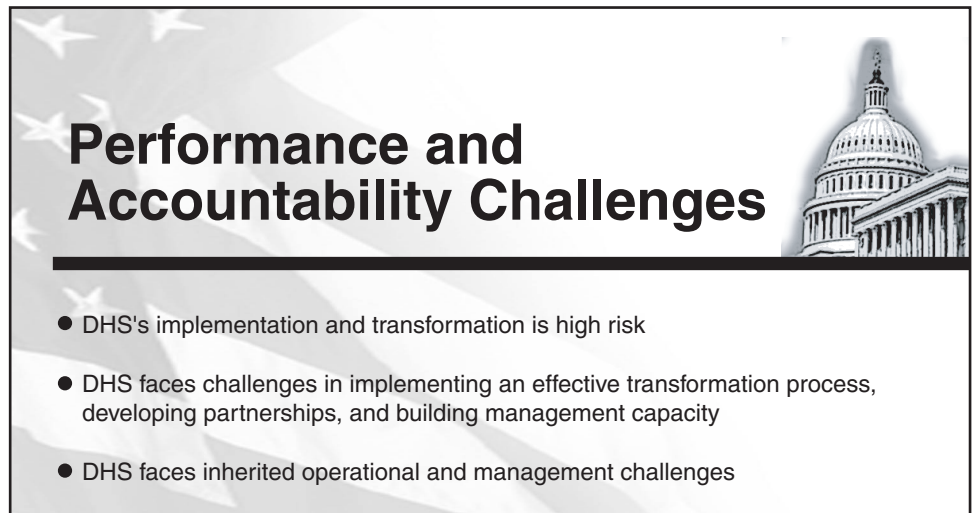
David M. Walker
Comptroller General
of the United States

Major Performance and Accountability Challenges

The November 2002 enactment of legislation creating the Department of Homeland Security (DHS) represents a historic moment of almost unprecedented action by the federal government to fundamentally transform how the nation will protect itself from terrorism.¹ Rarely in the country's past has such a large and complex reorganization of government occurred or been developed with such a singular and urgent purpose. The government now has a unique opportunity to transform a disparate group of agencies with multiple missions, values, and cultures into a strong and effective cabinet department whose goal will be to, among other things, protect U.S. borders, improve intelligence- and information-sharing activities, and prevent and respond to potential terrorists acts. Together with this unique opportunity, however, also comes significant risk to the nation that could occur if this implementation and transformation is not successful. A DHS that does not swiftly meet expectations for protecting America could increase the vulnerability of our borders, citizens, and economy, and not achieve anticipated effectiveness in operations.

This Performance and Accountability Series report on DHS provides an overview of the new department's challenges as it seeks to simultaneously establish itself and protect the nation from terrorism. This report is being issued as part of a special series of reports that discuss major management challenges and program risks across the government, including other reports highlighting issues affecting homeland security. This report raises issues that deal with both the broad transition and transformation concerns the department faces, and also the many specific program operational and management challenges that DHS will inherit from its component parts in such areas as border security and disaster mitigation.

¹ Pub. L. 107-296, Nov. 25, 2002.



Performance and Accountability Challenges

- DHS's implementation and transformation is high risk
- DHS faces challenges in implementing an effective transformation process, developing partnerships, and building management capacity
- DHS faces inherited operational and management challenges

Implementing and Transforming the New Department of Homeland Security Is High Risk

We believe that the implementation and transformation of DHS is a high risk, and we have added it to our 2003 High Risk List. This designation is based on three factors. First, the implementation and transformation of DHS is an enormous undertaking that will take time to achieve in an effective and efficient manner. Second, DHS' prospective components already face a wide array of existing management and operational challenges. Finally, failure to effectively carry out its mission exposes the nation to potentially very serious consequences.

In the aftermath of September 11, 2001, invigorating the nation's homeland security missions has become one of the federal government's most significant challenges. DHS, with an anticipated budget of almost \$40 billion and over 170,000 employees, will be the third largest government agency; not since the creation of the Defense Department more than 50 years ago has the government sought to integrate and transform something of this magnitude. In the Defense Department's case, the effective transformation took many years to achieve and, even today, the department continues to face enduring management challenges and high risk areas that are, in part, legacies to its unfinished integration.

Effectively implementing and transforming DHS may be an even more daunting challenge. The Defense Department, at least, was formed almost entirely from agencies whose principal mission was national defense. DHS will combine 22 agencies specializing in various disciplines, including law

enforcement, border security, biological research, computer security, and disaster mitigation, for instance. Further, DHS will take on some non-homeland security activities, such as the Coast Guard's marine safety responsibilities and the Federal Emergency Management Agency's (FEMA) natural disaster response functions. Yet, only in the effective integration and collaboration of these entities will the nation achieve the synergy that can help provide better security against terrorism. The magnitude of the responsibilities, combined with the challenge and complexity of the transformation, underscore the perseverance and dedication that will be required of all of DHS' leaders, employees, and stakeholders to achieve success.

Further, it is well recognized that mergers of this magnitude in the public and private sector carry significant risks, including lost productivity and inefficiencies. Generally, successful transformations of large organizations, even those undertaking less strenuous reorganizations and with less pressure for immediate results, can take from 5 to 7 years to achieve. Necessary management capacity, communication and information systems, as well as oversight mechanisms must be established. Moreover, critical aspects of DHS' success will depend on well-functioning relationships with third parties that will take time to establish and maintain, including those with other federal agencies with homeland security responsibilities, such as the State Department, the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), the Defense Department, and the Departments of Health and Human Services (HHS) and Transportation (DOT); state and local government; and the private sector. Creating and maintaining a structure that can leverage partners and stakeholders will be necessary to effectively implement the national homeland security strategy.

The new department also is being formed from components with a wide array of existing major management challenges and program risks. For instance, one DHS directorate's responsibility includes the protection of critical information systems—an area that GAO already considers a high risk. In fact, many of the major components merging into the new department, including the Immigration and Naturalization Service (INS), the Transportation Security Administration (TSA), Customs Service, FEMA, and the U.S. Coast Guard, face at least one major management problem such as strategic human capital risks, information technology management challenges, or financial management vulnerabilities. They also confront an array of program operations challenges and risks. For example, TSA has had considerable challenges in meeting deadlines for

screening baggage, and the agency has focused most of its initial security efforts primarily on aviation security and is working with other agencies towards defining the roles and responsibilities for surface transportation security. INS has had difficulty tracking aliens due to unreliable address information. Customs must meet challenges from the potential threats of weapons of mass destruction smuggled in cargo arriving at U.S. ports, and the Coast Guard faces the challenges inherent in a massive fleet modernization.

DHS's national security mission is of such importance that the failure to address its management challenges and programs risks could have serious consequences on our intergovernmental system, our citizens' health and safety, and our economy. Overall, our designation of DHS as a high risk area and its inclusion on the 2003 High Risk List stems from the importance of its mission and the nation's reliance on the department's effectiveness in meeting its challenges for protecting the country against terrorism.

Implementation and Transformation Challenges

The creation of DHS is an enormous management challenge. The size, complexity, and importance of the effort make the challenge especially daunting and incomparably critical to the nation's security. Building an effective department will require consistent and sustained leadership from top management to ensure the needed transformation of disparate agencies, programs, and missions into an integrated organization. To achieve success, the end result should not simply be a collection of components in a new department, but the transformation of the various programs and missions into a high performance, focused organization. The new department will need to build a successful transformation that instills the organization with important management principles, rapidly implements a phased-in transition plan, leverages the new department and other agencies in executing the national homeland security strategy, and builds collaborative partnerships with federal, state and local, and private sector organizations. Management capacity and an accountability structure should be built to ensure continuity and achieve goals. Actions that must be taken to ensure the success of DHS over the long term include:

- a comprehensive transformation process,
- strong partnerships,
- management capacity, and

- performance, objectives, key milestones and an oversight structure.

Comprehensive Transformation Process

The creation of DHS represents one of the largest and most complex restructurings in the federal government. To improve opportunities for success, DHS's leadership can gain important perspectives from the lessons learned and best practices of other organizations that have been involved in significant mergers and transformations. Indeed, major mergers and acquisitions in the private sector often do not live up to their expectations or potential. Moreover, in the short term, the experience of major private sector mergers and acquisitions is that productivity and effectiveness actually decline. This happens for a number of reasons. For example, attention is concentrated on critical and immediate integration issues and diverted from longer-term mission issues. In addition, employees and managers inevitably worry about their place in the new organization. The key is to adopt practices that minimize the duration and the significance of factors that reduce productivity and effectiveness and ultimately to create an organization that is more than the “sum of its parts.”

On September 24, 2002, GAO convened a forum of public and private sector leaders to discuss useful practices from major private and public sector organizational mergers, acquisitions, and transformations that federal agencies could learn from to successfully transform their cultures and DHS could use to merge its various originating components.² The results of this forum provide insights into the challenges facing the federal government in forming a new cabinet department and in building a high performance organization.

Figure 1 below and the following sections outline key practices identified in the forum that can serve as a guide to DHS as it seeks to transform and meld disparate cultures in response to governance challenges.

² U.S. General Accounting Office, *Highlights of a GAO Forum: Mergers and Transformation: Lessons Learned for a Department of Homeland Security and Other Federal Agencies*, [GAO-03-293SP](#) (Washington, D.C.: Nov. 14, 2002).

Figure 1: Lessons Learned Regarding Mergers and Transformations for DHS

- Ensure top leadership drives the transformational change.
- Establish a coherent mission and integrated strategic goals to guide the transformation.
- Focus on a key set of principles and priorities at the outset of the transformation.
- Set implementation goals and a timeline to build momentum and show progress from day one.
- Dedicate an implementation team to manage the transformation process.
- Use the performance management system to define responsibility and assure accountability for change.
- Establish a communication strategy to create shared expectations and report related progress.
- Involve employees to obtain their ideas and gain their ownership for the transformation.
- Build a world-class organization.

Source: GAO.

Leadership, mission and goals, and priorities: Leadership is critical. By its very nature, the transformation process entails fundamental change. Consistent leadership helps the transformation process stay on course and can help bridge the differences in leadership and management styles among the originating components. Top leadership must set priorities and focus on the most critical issues. While top leadership is indispensable, it also will be important to have a management team dedicated to the transformation process to ensure changes are thoroughly implemented and sustained over time.

The mission and strategic goals of an organization must become the focus of the transformation, define the culture, and serve as a vehicle to build employee and organizational identity and support. Mission clarity and a clear articulation of priorities will be critical, and strategic goals must align with and support the mission and serve as the continuing, visible guideposts for decision making. The Homeland Security Act of 2002³ states that the DHS mission includes preventing terrorist attacks within the United States, reducing America's vulnerability to terrorism, and minimizing the damage and assisting in the recovery from attacks that do occur. In addition, DHS will assume many non-homeland security responsibilities, making it important for the department to clearly articulate short- and long-term goals and integrate these diverse missions into a strategic goal framework. Top leaders have a critical role in setting policy and goals, but management and employees must also be involved and support the strategic goals in order to effectively understand and work to achieve the department's mission.

In establishing DHS' strategic goals, the new department's leadership also needs to address the National Strategy for Homeland Security, which articulates the administration's plans for preventing and responding to terrorism. DHS has a key role to play in implementing the national strategy, which provides a definition of homeland security and sets forth overarching goals. Although the strategy is an important contribution to homeland security efforts, many of the implementation plans and activities for achieving these goals are not yet developed, such as establishing meaningful performance measures and articulating clear roles and responsibilities. Through its own goal and priority setting, DHS can make the national strategy much more robust and comprehensive.

In bringing together various programs and missions, the new organization must have a clear set of principles and priorities that serve as a framework to help the organization create a common culture and establish organizational and individual expectations. Principles are the core values of an organization—they can help DHS to define the attributes that are intrinsically important to what the new organization does and how it will do it. Additionally, priorities related to both the mission and the transition must be developed, to ensure appropriate sequencing of activities and alignments. These priorities provide the direction for implementing the new organization and for DHS' initial mission accomplishments.

³ Pub. L. 107-296, Nov. 25, 2002.

Implementation goals, timeline, and resources: Since a successful transformation process often takes 5 or more years to complete, it is essential to establish action-oriented implementation goals and a timeline with milestone dates to track the organization's progress towards its intermediate and long-term transformation goals. By demonstrating progress towards these transformation goals, the organization builds momentum and demonstrates that real progress is being made. In addition, having implementation goals and milestone dates helps pinpoint performance shortfalls and gaps and suggests midcourse corrections, including any needed adjustments to the organization's future goals and milestones.

Dedicated resources are critical to the successful management of the transformation process. A strong and stable implementation team that will be responsible for the transformation's day-to-day management can be an important vehicle to ensuring that the implementation and transformation of the new department receive the focused, full-time attention needed to sustain a successful effort. The implementation team can ensure that the various change initiatives are sequenced and implemented in a coherent and integrated way and that employees and other stakeholders are kept informed. Such a team must have direct access and be accountable to top leadership. At the same time, the team must be given the necessary authority and resources to carry out its responsibilities.

Transition planning efforts for DHS have been started, but more sustained efforts will be necessary. In November 2002, the administration, as required by law, submitted a Department of Homeland Security Reorganization Plan to the Congress.⁴ The plan provides information on the transfer of agencies, personnel, assets, and obligations to DHS and any consolidation, reorganization, and streamlining of agencies transferred to DHS as a result of the legislation. In complying with the legislation requiring the reorganization plan, the administration has identified the basic functions that will be transferred to DHS and provided some initial dates for transferring the incoming organizational entities. However, the transition plan is limited in its description of actions and activities that will be necessary, and it does not reflect the full range of actions that must occur in order to achieve an effective integration of agencies, programs, and missions into the new department. More comprehensive planning is needed that addresses the specifics of melding the new department's people, strategies, systems, and processes in a smooth and integrated manner. Issues that need to be addressed range from how the department will move to a single payroll system and what that system will be; to how border entry points should function—who operates the entry points, what do they do, what are their support systems. We believe that a more comprehensive transition plan will be necessary, one that addresses the full transition period and includes the identification of key activities and milestones to transform DHS into a fully integrated, high performance organization, and establishes accountability for achieving results.⁵

Employee involvement, communication, and performance: People will determine the success of DHS and the transformation that must be achieved. A change of culture is at the heart of a successful transformation—and DHS is no exception. The importance of redefining the organizational culture should not be avoided, but rather must be aggressively addressed at the outset and throughout the transformation process. Employee involvement, communication, and performance management will be critical to this process.

Employee involvement is critical from the beginning of the transformation process in order to achieve employee ownership of the changes. Further, it

⁴ *Department of Homeland Security Reorganization Plan* (The White House, Washington, D.C.: Nov. 25, 2002).

⁵ U.S. General Accounting Office, *Homeland Security: Management Challenges Facing Federal Leadership*, [GAO-03-260](#) (Washington, D.C.: Dec. 20, 2002).

strengthens the transformation process by including frontline perspectives and experiences. However, organizations and their employees must guard against being so involved in implementing their transformation initiatives that they lose sight of the fundamental reason for the transformation—improved results.

An effective and ongoing internal and external communication strategy is essential to making the transformation occur. Communication is not just about “pushing the message out,” but it should facilitate a two-way honest exchange with and allow for feedback from employees, customers, and stakeholders. This communication is central to forming the effective internal and external partnerships that are vital to the success of any organization.

A communication strategy is especially crucial in the public sector, where policymaking and program management demand transparency and a full range of stakeholders and interested parties are concerned not only with what results are to be achieved, but also what processes are to be used to achieve those results. This demand for transparency is a fact that needs to be accepted in any public sector transformation.

Finally, a performance management system can help manage and direct the transformation process. The performance management system must create a “line of sight” showing how team, unit, and individual performance can contribute to overall organization results. The system serves as the basis for setting expectations for employees’ roles in the transformation process. It also evaluates individual performance and contributions to the success of the transformation process and ultimately, organizational results.

Building a world-class organization: The formation of DHS is an important step in the federal government’s effort to improve homeland security. In establishing a results-oriented culture that can reach its full potential, the organization and its leaders should carefully select the best solution for the new organization. It will be important to have key positions filled with people who possess the critical competencies needed by the organization. Further, systems and processes need to be tailored to the organization. Best practices in systems and processes should be sought wherever they may be found. The best solution may not be to adopt the approaches or systems used by the largest component.

Building Strong Partnerships

The consolidation of many agencies, programs, and missions into DHS is designed, in part, to improve coordination and collaboration of organizations with homeland security missions. DHS must establish effective mechanisms to strengthen the ability of its many entities to share information and build partnerships that yield results and help meet national homeland security objectives.

Even with the consolidation of many entities into DHS, there still remain a significant number of federal agencies or mission areas that are not being incorporated into the new department but which still need to be integrated into the overall homeland security strategy. Agencies such as the FBI, CIA, and the U.S. Marshals Service, for example, have important roles to play—especially in information sharing and intelligence activities—and their efforts must be coordinated with DHS to ensure effective and efficient action. DHS must effectively coordinate with the State Department on visa processing, with HHS on smallpox vaccination preparations and public health preparedness, and with many other agencies that are not being incorporated into the new organization.

Likewise, DHS will need to establish effective collaboration with the Defense Department, which also has a growing role to play in homeland security. In 2002, the President approved the latest Defense Department Unified Command Plan intended to realign and streamline the U.S. military structure to better address 21st century threats. Characterized as the most significant reform of the nation's military command structure since the first command plan was issued shortly after World War II, the plan, among other things, establishes the U.S. Northern Command (NORTHCOM), responsible for land, aerospace, and sea defenses of the United States. Its geographic area includes the continental United States, Alaska, Canada, Mexico, portions of the Caribbean, and the contiguous waters in the Atlantic and Pacific oceans.

Achieving national preparedness and response goals hinges on the federal government's ability to form effective partnerships with nonfederal entities. Although collaboration with state and local governments and the private sector is increasing, more needs to be done in order to enhance its effectiveness. DHS has a strong role to play in achieving this objective. Prior to September 11, 2001, the public and private sectors collaborated on homeland security activities, but the catastrophic events heightened the recognition that more concrete and long-term approaches were necessary. The new department needs to gain the full participation and buy-in of

partners in both policy formulation and implementation to develop effective partnerships.

The new DHS legislation contains provisions that should help maintain coordination among public sector entities by establishing within the DHS' Office of the Secretary an Office for State and Local Coordination that will coordinate DHS activities relating to state and local government. In addition, this office is tasked with developing a process for receiving meaningful input from state and local governments on furthering the national strategy for combating terrorism and other homeland security activities. DHS also includes an Information Analysis and Infrastructure Protection Directorate that will have responsibility for assessments and protection plans for key resources and critical infrastructure. Part of that effort will include consultation and cooperation with state and local governments and the private sector. For example, the directorate will recommend protection measures in cooperation with state and local government agencies and authorities and the private sector.

The DHS legislation and existing coordinating mechanisms provide a base for fully developing a partnership structure that provides maximum leverage of resources and information. Effectively implementing a strong partnership network is critical to accomplishing DHS' homeland security mission.

Building Management Capacity

The multiple mission responsibilities of the new department will require significant management capacity to ensure that DHS can successfully transform the various agencies, programs, and missions into a strong and effective organization. The new department must grapple not only with operational issues that will require immediate attention to better secure our borders or to enhance information sharing, but to also create a well run, sustainable department for the long term.

In our July 17, 2002, testimony entitled *Homeland Security: Critical Design and Implementation Issues* ([GAO-02-957T](#)), we identified certain critical success factors a new organization such as DHS should emphasize in its initial implementation phase. Over the years GAO has made observations and recommendations about many of these success factors, including human capital, information technology management, acquisition management, financial management, and several other important tools critical to building and sustaining effective organizations. The full list of success factors is described on page 32.

The DHS legislation created an Under Secretary for Management, who will be responsible for the management and administration of the department. The effectiveness of this position will be critical to the department's performance. Essentially, the person should function as a chief operating officer (COO). A COO can provide the sustained management attention essential for addressing key infrastructure and stewardship issues, while helping to facilitate the transition and transformation process. This position can be the focal point for building and sustaining management capacity. The Secretary and Deputy Secretary can then focus their efforts on policy and strategic issues. To be successful, the Under Secretary must be given the necessary authority to successfully lead departmentwide initiatives. Further, the person filling this position should have the demonstrated leadership skills in managing large and complex organizations and experience achieving results in connection with "good government" responsibilities and initiatives.

With respect to human capital, DHS will face significant challenges that will require a comprehensive strategy capable of ensuring the new department can acquire, develop, and retain the skills and talents needed to prevent and protect against terrorism. This will require identifying skill needs; attracting people with scarce skills, such as language proficiency, into government jobs; melding diverse compensation systems that can support the new department's many needs; and establishing a results-oriented, accountable culture that can meet national goals and priorities. An environment that promotes employee involvement and empowerment, as well as constructive and cooperative labor-management relations, will be critically important. The various unions whose members are slated to become employees of DHS will, together with the department's leadership, need to work in unity of purpose to achieve the goals of transforming DHS and strengthening national security.

Moreover, agencies slated to move into DHS have long-standing human capital problems that will need to be addressed. One of these challenges has been the ability to hire and retain a talented and motivated staff. For example, We have reported that INS has been unable to reach its program goals in large part because of such staffing problems as hiring shortfalls and agent attrition.⁶ Several INS functions have been impacted by the lack of a staff resource allocation model to identify staffing needs.⁷ Therefore, it is likely that increased attention to the enforcement of immigration laws and border control will test the capacity of DHS to hire large numbers of inspectors for work at our nation's border entry points. Other agencies being integrated into DHS are also expected to experience challenges in hiring security workers and inspectors. For example, the Agriculture Department's Animal and Plant Health Inspection Service (APHIS) has been seeking to increase the size of its inspection force by 50 percent at the same time that the Customs Service, INS, and other agencies are increasing the size of their inspection staffs.⁸

The DHS legislation provided certain human capital flexibilities in order to establish a contemporary human capital system to better meet the needs of the new department. These flexibilities can be important tools in addressing the department's pressing human capital needs, including recruiting, retaining, and aligning staff. DHS should consider the six key practices for the effective use of human capital flexibilities that we identified as part of a recent review.⁹ In addition, DHS should look to other agencies that have been given flexibilities in the past—the Defense Department, the Internal Revenue Service, TSA—to learn and build on their experiences to achieve the maximum benefit. As required by the legislation, there also needs to be transparency and accountability in designing the system, involving stakeholders—particularly employees—and keeping the Congress informed. These human capital flexibilities can greatly benefit the department, but only if properly used.

⁶ U.S. General Accounting Office, *Immigration Enforcement: Challenges to Implementing the INS Interior Enforcement Strategy*, [GAO-02-861T](#) (Washington, D.C.: June 19, 2002).

⁷ U.S. General Accounting Office, *Immigration and Naturalization Service: Overview of Recurring Management Challenges*, [GAO-02-168T](#) (Washington, D.C.: Oct. 17, 2001).

⁸ [GAO-03-260](#).

⁹ U.S. General Accounting Office, *Human Capital: Effective Use of Flexibilities Can Assist Agencies in Managing Their Workforces*, [GAO-03-2](#) (Washington, D.C.: Dec. 6, 2002).

Improving information technology management will also be critical to transforming the new department. Not only will DHS face considerable challenges in integrating the many systems and processes that provide management with decision information, but it must sufficiently identify its future needs in order to build effective systems that can support the national homeland security strategy in the coming years. The Office of Management and Budget (OMB), in its current reexamination of ongoing technology and management information systems, has taken an initial first step to evaluate the new department's component systems. Much more needs to be done, however, before DHS can achieve the needed systems integration, including the development and implementation of an enterprise architecture, or corporate blueprint, to guide its information technology investments. Other key information technology management capacities that DHS will need to establish include effective computer security, investment management processes, and system and service acquisition management practices.

Several of the agencies being incorporated into DHS will bring the new department inherited information technology problems. For instance, INS has had long-standing difficulty developing and fielding information systems to support its program operations. Since 1990, we have reported that INS managers and field officials did not have adequate, reliable, and timely information to effectively carry out the agency's mission. For example, INS' benefit fraud investigations have been hampered by a lack of integrated information systems.¹⁰ Because INS' four service centers investigating benefit fraud operate different information systems that do not interface with each other, INS officers may be making decisions without routine access to significant information, resulting in benefits being granted to individuals not entitled to receive them. More recently, INS's alien address information could not be fully relied on to locate many aliens who were believed to be in the country and who might have knowledge that would assist the nation in its antiterrorism efforts.¹¹ Contributing to this situation was INS' lack of written procedures and automated controls to help ensure that reported changes of address by aliens are recorded in all of INS' automated databases. Our work has

¹⁰ U.S. General Accounting Office, *Immigration Benefit Fraud: Focused Approach Is Needed to Address Problems*, [GAO-02-66](#) (Washington, D.C.: Jan. 31, 2002).

¹¹ U.S. General Accounting Office, *Homeland Security: INS Cannot Locate Many Aliens Because It Lacks Reliable Address Information*, [GAO-03-188](#) (Washington, D.C.: Nov. 21, 2002).

identified weaknesses in INS' information technology management capacities as the root cause of its system problems, and we have made recommendations to correct the weaknesses. INS has made progress in addressing our recommendations.

Much also remains to be done to strengthen the government's ability to leverage information sharing between and among important government and private sector stakeholders. The success of the national homeland security strategy relies on the ability of all levels of government and the private sector to communicate effectively with one another. Activities that are hampered by organizational fragmentation, technological impediments, or ineffective collaboration blunt the nation's collective efforts to prevent or minimize terrorist acts.

DHS will be faced with the challenge of integrating the procurement functions of many of its constituent programs and missions. Early attention to strong systems and controls for acquisition and related business processes will be critical both to ensuring success and maintaining integrity and accountability. Several of the incoming agencies, such as Customs and the Coast Guard, have major procurement programs under way that must be closely managed to ensure they achieve expectations. Inherited challenges exist in several agencies. Despite some progress, Customs still lacks important acquisition management controls.¹² For its new import processing system, Customs has not begun to establish process controls for determining whether acquired software products and services satisfy contract requirements before acceptance, nor to establish related controls for effective and efficient transfer of acquired software products to the support organization responsible for software maintenance. Agreeing with one of our recommendations, Customs continues to make progress and plans to establish effective acquisition process controls.

¹² U.S. General Accounting Office, *Customs Service Modernization: Management Improvements Needed on High-Risk Automated Commercial Environment Project*, GAO-02-545 (Washington, D.C.: May 13, 2002).

With respect to financial management, the new department has a stewardship obligation to prevent fraud, waste, and abuse, to use tax dollars appropriately, and to ensure financial accountability to the President, the Congress, and the American people. DHS can only meet these goals if it establishes systems, processes, and controls that help to ensure effective financial management. DHS must also insist on the adherence of strong financial principles for its incoming agencies, many of which have ongoing challenges in their systems, processes, or internal controls over financial information. For instance, FEMA received a qualified opinion on its financial statements following its fiscal year 2001 financial audit, and it has a number of material internal control weaknesses.¹³ For fiscal year 2001, INS received its first unqualified opinion on its financial statements. However, it took significant effort to achieve this opinion and the auditors reported several material internal control weaknesses. DOT, from which several DHS agencies are coming, has financial management deficiencies, including with its accounting system. In addition to addressing the many ongoing challenges existing in the programs of incoming agencies, DHS will need to focus on building future systems as part of its enterprise architecture approach to ensure an overarching framework for the agency's integrated financial management processes. Plans must be developed and implemented to bridge the many financial environments in which incoming agencies currently operate to an integrated DHS system.

Successful financial management of homeland security will also be dependent on greater budgetary transparency and a level of detail that provides useful information for congressional budget deliberations and executive decision making. Collaboration and coordination will be critical to avoiding duplicative or wasteful spending on homeland security, both within DHS as well as among other agencies that have homeland security missions. DHS will need to work with OMB and the Congress to achieve the needed level of transparency as funding is transferred or merged to ensure that intended results are achieved and funds are effectively leveraged.

DHS is also expected to extensively utilize third parties, including state and local governments and the private sector, to meet national homeland

¹³ U.S. General Accounting Office, *U.S. Government Financial Statements: FY 2001 Results Highlight the Continuing Need to Accelerate Federal Financial Management Reform*, [GAO-02-599T](#) (Washington, D.C.: Apr. 9, 2002).

security goals. Through a variety of important tools, including grants and regulations, tax incentives, and other activities, as well as the purchase of goods and services, the new department must not only ensure that the tools it uses are the most appropriate for the situation but that it also receives the intended benefit. Through effective program and financial management, DHS will need to build strong oversight mechanisms to ensure that third party obligations are met.

Establishing Performance Milestones and Oversight for DHS

The new department, in fulfilling its broad mandate, has the challenge of developing a national homeland security performance focus, which relies on related national and agency strategic and performance planning efforts of the Office of Homeland Security (OHS), OMB, and other departments and agencies. Indeed, the planning activities of the various departments and agencies represent a good start in the development of this focus; however, our past work on implementation of the Government Performance and Results Act has highlighted ongoing difficulty with many federal departments and agencies setting adequate performance goals, objectives, and targets. Accordingly, attention is needed to developing and achieving appropriate homeland security performance expectations and measures and in ensuring that there is linkage between DHS, other agency plans, and the national strategy. Ensuring these capabilities and linkages will be vital in establishing a comprehensive homeland security planning and accountability framework that will not only guide the nation's homeland security efforts but also help assess how well they are really working.

The new DHS legislation does require some specific planning efforts that include goals and measures. For example, the Directorate of Science and Technology is to develop a national policy and strategic plan for developing countermeasures to weapons of mass destruction. The directorate must develop comprehensive, research-based definable goals and annual measurable objectives and specific targets to evaluate the goals.

Accountability is also a critical factor in ensuring the success of the new department. The oversight entities of the executive branch, including OMB and OHS, will have a vital role to play in ensuring expected performance and accountability. As stated in the President's June 2002 DHS proposal, OHS is seen as continuing to play a key role in advising the President and coordinating a simplified interagency process. Likewise, congressional committees, with their long-term and broad institutional roles, will also play a role in overseeing the transformation of the federal government as it

meets the demands of its homeland security mission. The creation of DHS has raised questions regarding how the Congress can best meet its oversight, authorization, and appropriations responsibilities for the new department. DHS will be comprised of some 22 federal agencies or their components overseen by numerous congressional committees of jurisdiction. In recognizing this complexity, the DHS legislation instructs both Houses of Congress to review their committee structures in light of the reorganization of homeland security responsibilities within the executive branch. As a result, the Congress has begun to explore ways to facilitate conducting its responsibilities in a more consolidated and integrated manner. During this period of transformation, the Congress may need to periodically reassess its structure to maximize the effectiveness of its DHS oversight.

Addressing Significant Program Operational and Management Challenges

In addition to the high risk associated with implementing and transforming a new department from the multitude of agencies and activities, DHS' leadership will be confronted with a number of operational and management challenges emanating from the functions and organizations being transferred to it. We have identified a number of major operational and management challenges in the programs and missions being transferred into the department. These challenges are discussed in depth in our Performance and Accountability reports on their current departments and in other GAO work on homeland security. However, to provide a comprehensive assessment of the new department, summaries of these risks and challenges follow.

Information Analysis and Infrastructure Protection

Within DHS, a new directorate is responsible for accessing, receiving, and analyzing law enforcement information, intelligence information, and other information from agencies of federal, state, and local governments and the private sector, and to integrate such information to identify and assess the nature and scope of terrorist threats. The new directorate's role also includes the protection of the nation's critical information systems. In a separate report, we have designated protecting information systems supporting the federal government and the nation's critical infrastructures as a governmentwide high risk. Because of the new department's central role in this issue, resolution of this high risk will, in part, be a responsibility and significant challenge for DHS.

Since 1997, we have designated information security as a governmentwide high-risk issue. This year, we have expanded the high-risk issue to emphasize the increased importance of protecting the information systems that support critical computer infrastructure such as national defense, power distribution, and water supply.¹⁴ Terrorist attacks and threats have further underscored the need to manage critical infrastructure protection (CIP) activities that enhance the security of the cyber and physical public and private infrastructures that are essential to national security, national economic security, and/or national public health and safety.

At the federal level, cyber CIP activities are perhaps the most critical component of a department or agency's overall information security program. In addition, although the government has made steady progress in working with the private sector to better secure critical infrastructures, this issue is also designated as part of our information security high-risk issue because:

- the failure to adequately protect these infrastructures could have consequences for national and economic security and /or national public health and safety,
- terrorist groups and others have stated their intentions of attacking our critical infrastructures,
- federal influence over the private sector's management of our nation's critical infrastructure poses unique challenges, and
- further actions on GAO's CIP recommendations are needed.

¹⁴ U.S. General Accounting Office, *High-Risk Series: An Update*, [GAO-03-119](#) (Washington, D.C.: January 2003).

A number of significant actions have taken place to better position the nation to protect our critical infrastructures, including issuance of (1) Presidential Decision Directive 63, which described a strategy for cooperative efforts by government and the private sector and established organizations to provide central coordination and support, (2) Executive Order 13231, which established the President's Critical Infrastructure Protection Board, and (3) a comment draft of a *National Strategy to Secure Cyberspace*.¹⁵

Although the actions taken to date are major steps to more effectively protect our nation's critical infrastructures, we have identified and made numerous recommendations over the last several years concerning CIP challenges that still need to be addressed. For each of these challenges, improvements have been made and continuing efforts are in progress. However, much more needs to be done. These challenges include developing a national CIP strategy, improving analysis and warning capabilities, and improving information sharing on threats and vulnerabilities.

Moreover, the transformation of the FBI at the same time as the formation of DHS will add an additional level of complexity to the challenge of ensuring effective coordination, communication, and sharing of information. In previous work, we have noted that changes in the FBI must be part of, and consistent with, broader governmentwide transformations that are taking place.¹⁶ As a result, the FBI needs to develop a comprehensive transformation plan with key milestones and assessment points to guide its overall transformation efforts. With the FBI as a key partner, it will be important for DHS to be aware of ongoing changes at the FBI and assess their impact on its operations and the integration of activities between the two agencies.

Border and Transportation Security

The new Border and Transportation Security Directorate faces considerable challenges and its success will require sustained attention

¹⁵The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace—For Comment Draft*, September 2002.

¹⁶ U.S. General Accounting Office, *FBI Reorganization: Initial Steps Encouraging but Broad Transformation Needed*, [GAO-02-865T](#) (Washington, D.C.: June 21, 2002).

from the new department's leadership. The operational and management challenges include:

- **Customs Service:** As a result of the homeland security legislation, the Customs Service will be transferred to DHS from the Treasury Department. However, the Secretary of the Treasury will retain authority over customs revenue functions. The splitting of revenue functions from other authorities will initially pose a challenge to developing clarity in roles and responsibilities and effective, efficient, and seamless operations. Further, in our report on the Treasury Department, we have identified improving Customs' management of multiple missions as a performance and accountability challenge. Customs has the dual missions of enforcing laws to safeguard borders against illegal entry of goods and of regulating legitimate commercial activity. While September 11 has focused Customs on keeping out of the country any "implements of terrorism," such as chemical, biological, or nuclear materials that could be used as weapons, the agency still faces challenges associated with trade compliance and overall border security.

Our recently completed and ongoing work has identified additional challenges that directly or indirectly affect Customs' efforts to improve security at U.S. borders to safeguard against the illegal entry of goods, including potentially harmful, hazardous, or otherwise illegal commodities. These challenges include improving different international mail and package inspections processes, ensuring that various illegal items, including weapons of mass destruction, do not enter the country in cargo containers at seaports, and acquiring a new import processing system. According to Customs, the inspection of incoming foreign mail remains largely a manual process that relies primarily on physical examination. One courier is working with Customs to pilot test an advance manifest system, a computerized database that receives cargo manifest information. The database will allow Customs to analyze incoming package information and make more informed decisions about what packages to inspect. Since our work on international mail and containerized cargo processing¹⁷ involves information that Customs considers to be law enforcement sensitive, we are precluded from further discussing the challenges posed by mail and cargo processing in this unclassified report.

¹⁷ The Committee on Energy and Commerce, House of Representatives requested this work.

Whatever their nature, Customs' challenges could likely be complicated during its proposed transition to the new Department of Homeland Security.

- **Transportation Security Administration:** We have identified transportation security as a performance and accountability challenge for the Departments of Homeland Security and Transportation. As discussed in our DOT report, the transformation of transportation security in order to reduce the vulnerability of the nation's surface and air transportation systems to terrorism and other disruptions represents a significant challenge to the new department.¹⁸ On November 19, 2001, the Aviation and Transportation Security Act¹⁹ was enacted, which created TSA and defined its primary responsibility as ensuring security in all modes of transportation. DOT has worked to make urgent security improvements throughout its modal administrations while simultaneously organizing TSA to meet the longer-term challenge of implementing security improvements that will not excessively inhibit commerce and travel or interfere with other critical missions. Since its creation in November 2001, TSA has focused primarily on aviation security challenges and is working towards defining the roles and responsibilities for surface transportation security. Specifically, TSA is developing memoranda of understanding with the other modal administrations within DOT that are expected to delineate the lines of authority between the parties and establish the specific responsibilities of various parties for transportation security. TSA plans to complete the memoranda by March 1, 2003.

¹⁸ U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Transportation*, [GAO-03-108](#) (Washington, D.C.: January 2003).

¹⁹ Pub. L. 107-71.

There are also continuing challenges for aviation security. Despite an impressive start in building the infrastructure of a large organization, TSA still faces formidable short- and long-term challenges in aviation security. According to TSA, it met the November 2002 deadline by hiring and deploying over 40,000 passenger screeners to screen passengers at 429 commercial airports. In addition, TSA reports that it met the December 31, 2002, deadline to screen all checked baggage. TSA reports that it hired and deployed more than 20,000 of an estimated 22,000 baggage screeners as of mid-December 2002 to screen all checked baggage and that as of December 31, 2002, about 90 percent of all checked baggage will be screened using explosive detection systems or explosive trace detection equipment, and the remaining checked baggage will be screened using alternative means such as canine teams, hand searches, and passenger-bag matching. Nevertheless, significant challenges remain. As of mid-December 2002, TSA has installed only 239 of the estimated 1,100 explosive detection machines and 1,951 of the estimated 6,000 trace detection machines needed to screen baggage to meet baggage screening requirements in the Aviation and Transportation Security Act.

In addition to securing passenger carry-on luggage and checked luggage TSA faces other immediate challenges in securing cargo aboard commercial passenger and all-cargo aircraft. To address these challenges, we recommended that TSA develop a comprehensive plan for air cargo security that incorporates a risk management approach, includes a list of security priorities, and sets deadlines for completing actions. TSA agreed with this recommendation.²⁰

TSA faces numerous transportation security challenges over the long term. The agency must ensure that transportation security funding needs are identified and prioritized and costs are controlled. Moreover, TSA believes its current funding levels are inadequate. The agency estimates that it will need about \$4.8 billion in fiscal year 2003, but that revenues from the new passenger security fee will pay for only about one third (\$1.7 billion) of that amount. As a result, TSA will need a major cash infusion at a time when federal budget deficits are growing. TSA needs to establish effective coordination among the many public and private entities responsible for transportation security. The agency

²⁰ U.S. General Accounting Office, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, [GAO-03-344](#) (Washington, D.C.: Dec. 20, 2002).

must also ensure adequate workforce competence and staffing levels. TSA has experienced difficulty in hiring and training its screening workforce and continues to face issues with its compensation and performance management systems. Finally, standards define the level of security that is needed and the safeguards that should be in place to meet the identified needs. New standards are being developed in some modes and are being considered in other modes. In addition to continuing challenges in standard development, there also are challenges in standards' implementation.

- **Visa processing:** Another important element in border and transportation security is the improvement of the nation's visa processing system. In our report on the Department of State, we identify strengthening the visa process to help prevent terrorism as a performance and accountability challenge.²¹ Since the September 11 attacks, some changes have been introduced to strengthen visa processing. For example, State has, with the help of other agencies, almost doubled the names and information on persons in the lookout system. Although these actions have strengthened the visa process, opinions and practices among overseas posts continue to diverge regarding the authority of consular officers to deny questionable applicants a visa and the role of the visa process in ensuring national security. Opinions and practices also differ regarding the appropriate changes to individual posts' visa policies and procedures that need to be made given the need for heightened border security. We have made a number of recommendations to State to address urgent and fundamental operational and coordination issues, and the department has indicated that it has taken steps to implement a number of our recommendations. However, more needs to be done. In the creation of DHS, the Secretary for DHS has been given certain visa policy-making responsibilities. It will be critical for DHS and State to work together to address the underlying challenge in visa processing, ensure a smooth transfer of certain responsibilities, and integrate visa processing activities to maximize effectiveness as an antiterrorism tool.
- **Immigration:** Numerous challenges also face INS, which is being integrated into the new department. The Congress has continued to express concern about INS' ability to carry out its enforcement and

²¹ U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of State*, [GAO-03-107](#) (Washington, D.C.: January 2003).

service functions. Over the last several years the Congress has significantly increased budget and staffing at INS to help the agency deal with its considerable workload. In creating DHS, the Congress established within DHS the Bureau of Citizenship and Immigration Services to help improve the performance of these activities. Further, the Bureau of Border Security has responsibility for enforcement functions.

These actions have resulted in a significant change in responsibilities for carrying out immigration functions. However, additional challenges remain, and will have to be addressed by DHS. In a memorandum dated November 8, 2002, the DOJ Inspector General enumerated the top management challenges for INS. Many of these challenges parallel our reporting. In our performance and accountability report on DOJ, we identify the following challenges:

- effective use of INS resources is necessary to fully implement a border control strategy,
- fragmented and unfocused INS efforts must be improved to combat immigration benefit fraud,
- impediments to reducing unauthorized employment need to be overcome,
- improvements are needed in identifying and removing criminal aliens,
- shortcomings in alien anti-smuggling efforts need to be eliminated,
- problems managing INS's application workload must be corrected,
- problems coordinating with State Department's visa operations need attention, and
- weaknesses in information technology management must be corrected.

Our report on DOJ contains an extensive discussion of these issues and our related recommendations. However, several are highlighted here.

The Border Patrol has been responsible for preventing and deterring aliens from illegally entering the United States between ports of entry. We reported in August 2001 that INS's preliminary estimates indicated that gaining control of the southwest border could take at least 5 more years and between 11,700 and 14,000 Border Patrol agents, additional support personnel, and hundreds of millions of dollars in technology and infrastructure.²² Further, the Justice Department's Inspector General reported in 2002 that INS developed a northern border strategy in 2000, but implementation was initially delayed because of changes in administration and in INS leadership, and then overwhelmed by the events of September 11.²³ In response to September 11, INS accelerated deployment of personnel and resources to the northern border, including increasing the number of Border Patrol agents from 24 to 245 in fiscal year 2001.

Despite years of increasing budgets and staff, INS has continued to experience significant problems managing its workload of processing applications. As of October 2002, INS had an application backlog of 5.2 million applications, an almost five-fold increase since October 1994. We reported in May 2001 that better automation capability and a more streamlined application process would enable INS to provide improved levels of service.²⁴ In 2002, the President announced a \$50 million initiative to eliminate backlogs. It should be noted that despite the importance and prevalence of information technology (IT) systems in accomplishing organizational core missions, INS has not yet fully implemented effective controls for managing its IT resources, although it is working to do so. This will provide an added level of difficulty in addressing other management problems.

Emergency Preparedness and Response

The new department will include a directorate for emergency preparedness and response and will inherit challenges from FEMA and HHS. FEMA will

²² U.S. General Accounting Office, *INS' Southwest Border Strategy: Resource and Impact Issues Remain After Seven Years*, GAO-01-842 (Washington, D.C.: Aug. 2, 2001).

²³ U.S. Department of Justice, Office of the Inspector General, *Follow-up Report on Border Patrol's Efforts to Improve Northern Border Security (Redacted Version)*. Report No. I-2002-004 (Washington, D.C.: February 2002).

²⁴ U.S. General Accounting Office, *Immigration Benefits: Several Factors Impede Timeliness of Application Processing*, GAO-01-488 (Washington, D.C.: May 4, 2001).

be transferred to DHS, thus the department will have responsibility for both FEMA's homeland security and non-homeland security responsibilities. Currently a stand-alone agency, we have issued a separate report on FEMA in which four mission and management challenges are identified. These challenges are: (1) ensuring effective coordination of preparedness and response efforts, (2) enhancing provision and management of disaster assistance for efficient and effective response, (3) reducing the impact of natural hazards by improving the efficiency of mitigation and flood programs, and (4) resolving financial management weaknesses to ensure fiscal accountability.

The first challenge deals with preparing for and responding to terrorism and nonterrorism-related disasters. Although FEMA and its missions will be transferred to DHS, its homeland security and nonhomeland security missions will be under separate DHS directorates. Specifically, preparedness for terrorism disasters will be placed in the Border and Transportation Security Directorate and other preparedness and response efforts will be located in the Emergency Preparedness and Response Directorate. This divisional separation could complicate FEMA's historical all-hazards approach—a comprehensive approach focused on preparing for and responding to all types of disasters, either natural or manmade. Separation of preparedness and response activities among differing federal entities has been a recurring problem in the past, and while consolidation of these activities within DHS does achieve a measure of consolidation, the separation of disaster and emergency responsibilities across two directorates of the new department will present coordination challenges for the appropriate DHS undersecretaries.

With respect to enhancing the provision and management of disaster assistance for efficient and effective response, FEMA will be challenged to:

- improve its criteria for determining state and local eligibility to receive federal disaster assistance;
- assess whether broadened determinations of federal disaster assistance in response to the terrorist attacks may establish precedent for future disasters;
- build on lessons learned from charities' response to September 11, and enhance disaster assistance training and resource planning;
- enhance oversight of disaster assistance; and

- improve an existing information system before it is used as a building block for a multiagency disaster management web site.

With respect to natural hazards, two of FEMA's major efforts have been its mitigation programs and the National Flood Insurance Program. Concerns have been raised regarding the demonstration of cost effectiveness of some mitigation projects in these programs. For the National Flood Insurance Program, cumulative program costs exceeded income by about \$1.3 billion during fiscal years 1993 through 2001 because the program is not actuarially sound.

Finally, FEMA faces challenges in resolving financial management weaknesses. FEMA's financial management effectiveness has become a concern because it received a qualified audit opinion on its most recent financial statements due to inadequate accounting for property and unliquidated obligations. Additionally, auditors identified material internal control weaknesses and compliance issues requiring correction.

In addition to FEMA, HHS' Office of Emergency Response will be transferred to DHS. In our report on HHS, we identify strengthening preparedness for public health emergencies, including bioterrorism, as a performance and accountability challenge.²⁵ Ensuring that every community and each of the approximately 3,000 local health departments across the nation meets a basic standard of preparedness is a significant challenge. Our reports have found significant weaknesses in key elements of the public health infrastructure that are critical to emergency response at the state and local level. In addition, we have noted a lack of coordination among programs with responsibility for public health emergency preparedness at the local, state, and federal levels. The creation of DHS has the potential to streamline overall funding and oversight responsibilities for preparedness and response. However, key public health preparedness functions will remain with HHS, and will present coordination challenges to DHS.

Further, we note that HHS faces challenges in strengthening the public health infrastructure, as well as related aspects of the private-sector health care system. Areas requiring strengthening include laboratory capacity, infectious disease surveillance, hospital surge capacity, blood supply,

²⁵ U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Health and Human Services*, [GAO-03-101](#) (Washington, D.C.: January 2003).

communications, human capital, and research and development. Clearly, addressing these challenges will impact the success of DHS in achieving its mission. Coordination between the two departments will be critical.

Science and Technology

The new department's Directorate of Science and Technology will have a diverse set of responsibilities and its effectiveness will depend upon strong relationships with other federal departments. Several components of the Department of Energy will be transferred to the new directorate, as will the Department of Agriculture's Plum Island Animal Disease Center and the Defense Department's National Bio-Weapons Defense Analysis Center. In addition to its own research activities, DHS will have to collaborate with HHS, the Department of Energy, and others to ensure essential research is accomplished for homeland security activities. Achieving balance among competing priorities will present unique challenges. Science and technology activities often serve multiple purposes and, as we have indicated in recent testimony before the Congress,²⁶ collaboration between and among federal agencies will be important to the success of missions that serve dual purposes.

The integration of these components will present unique challenges, particularly as DHS moves to address important needs of homeland security. For instance, one potential area where the new department will play a role is biometric technology, which can be used in associating a person with travel documents such as visas and passports. When used at a border inspection, the biometric comparison can be used to help decide whether to admit a traveler into the United States. Before any decision is made to implement biometrics in a border control system, the benefits of the system must be weighed against its costs. The purpose of any biometrics initiative is to prevent the entry of travelers who are inadmissible to the United States. The costs of a biometric border control system will not be trivial. Important policy implications must be addressed in trade-offs between increasing security and the impact on areas such as privacy, economy, traveler convenience, and international relations.

²⁶ U.S. General Accounting Office, *Homeland Security: Critical Design and Implementation Issues*, [GAO-02-957T](#) (Washington, D.C.: July 17, 2002).

Coast Guard

The Coast Guard will also be transferred to DHS, but it will remain as an independent unit and will not be incorporated into any of the new directorates. In recent reports and testimonies, we raise issues regarding the need for the Coast Guard to balance multiple missions.²⁷ Additionally, in our report on DOT, we identify a performance and accountability challenge of enhancing aviation and Coast Guard acquisition management to maximize returns from investment of public funds in large, complex, high-cost procurements.²⁸ Our report noted that aging and obsolete equipment has limited the Coast Guard's ability to achieve its safety and security missions, and that the agency is undertaking a costly, complex, and long-term program, called the Deepwater Capability Replacement Project, to modernize and replace its aging ships and aircraft. In 2002, the Coast Guard awarded a \$17 billion contract and projected sustained funding needs of \$500 million a year (in 1998 dollars) over the next 2 to 3 decades to develop the Integrated Deepwater System. The Coast Guard is addressing many of the concerns we reported in our 2001 Performance and Accountability Series²⁹ report, but uncertainties still exist in key areas such as attaining stable, sustained funding over a 20- to 30-year period, and controlling costs, especially in the contract's later years.

Critical Success Factors for New Organizations

In our July 17, 2002, report entitled *Homeland Security: Critical Design and Implementation Issues*⁹ ([GAO-02-957T](#)), we identified certain critical success factors a new organization such as DHS should emphasize in its initial implementation phase. These factors are:

- **Strategic planning:** Leading results-oriented organizations focus on the process of strategic planning that includes involvement of stakeholders,

²⁷ U.S. General Accounting Office, *Coast Guard: Strategy Needed for Setting and Monitoring Levels of Effort for All Missions*, [GAO-03-155](#) (Washington, D.C.: Nov. 12, 2002); U.S. General Accounting Office, *Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will be Pivotal to Success*, [GAO-02-886T](#) (Washington, D.C. June 25, 2002); U.S. General Accounting Office, *Coast Guard: Budget and Management Challenges for 2003 and Beyond*, [GAO-02-538T](#) (Washington, D.C.: Mar. 19, 2002); U.S. General Accounting Office, *Coast Guard: Actions Needed to Mitigate Deepwater Project Risks*, [GAO-01-659T](#) (Washington, D.C.: May 3, 2001).

²⁸ U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Transportation*, [GAO-03-108](#) (Washington, D.C.: January 2003).

²⁹ U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Transportation*, [GAO-01-253](#) (Washington, D.C.: January 2001).

assessment of internal and external environments, and an alignment of activities, core processes, and resources to support mission-related outcomes.

- Organizational alignment: The organization of a new department should be aligned to be consistent with the goals and objectives established in the strategic plan.
- Communications: Effective communication strategies are key to any major consolidation or transformation effort.
- Building partnerships: One of the key challenges of this new department will be the development and maintenance of homeland security partners at all levels of the government and the private sector, both in the United States and overseas.
- Performance management: An effective performance management system fosters institutional, unit, and individual accountability.
- Human capital strategy: A new department must ensure that its missions are not adversely impacted by the government's pending human capital crisis, and that it can recruit, retain, and reward a talented and motivated workforce, which has required core competencies, to achieve its mission and objectives. The people factor is a critical element in any major consolidation or transformation.
- Information technology management: A new department should leverage enabling technology to enhance its ability to transform capabilities and capacities to share and act upon timely, quality information about terrorist threats.
- Knowledge management: A new department must ensure it makes maximum use of the collective body of knowledge that will be brought together in the consolidation.
- Financial management: A new department has a stewardship obligation to prevent fraud, waste, and abuse; to use tax dollars appropriately; and to ensure financial accountability to the President, the Congress, and the American people.
- Acquisition management: Early attention to strong systems and controls for acquisition and related business processes will be critical both to

ensuring success and maintaining integrity and accountability. As one of the largest federal departments, DHS will potentially have some of the most extensive acquisition requirements in government.

- Risk management: In setting goals, priorities, and implementation plans, risks must be understood and managed. The new department must be able to maintain and enhance current states of homeland security readiness while transitioning and transforming itself into a more effective and efficient structural unit. DHS will also need to immediately improve the government's overall ability to perform risk management activities that can help to prevent, defend against, and respond to terrorist acts.
- Change management: Assembling a new organization out of separate pieces and reorienting all of its processes and assets to deliver the desired results while managing related risks will take an organized, systematic approach to change. A new department will both require an executive and operational capability to encourage and manage change.

GAO Contacts

Subjects covered in this report	Contact person
National preparedness	Randall Yim, Managing Director National Preparedness (202) 512-3580 yimr@gao.gov
Management challenges for homeland security	Patricia A. Dalton, Director Strategic Issues (202) 512-6806 daltonp@gao.gov
Transforming transportation security	John H. Anderson, Jr. Managing Director Physical Infrastructure Issues (202) 512-2834 andersonj@gao.gov
Information security issues and critical infrastructure protection	Robert F. Dacey, Director Information Technology (202) 512-3317 daceyr@gao.gov
Better manage programs designed to support state and local efforts to reduce crime	Laurie E. Ekstrand, Director Justice Issues (202) 512-8777 ekstrandl@gao.gov
Strengthen the visa process of as an antiterrorism tool	Jess T. Ford, Director International Affairs and Trade (202) 512-4268 fordj@gao.gov
Coordination of preparedness and response efforts	JayEtta Hecker, Director Physical Infrastructure (202) 512-2834 heckerj@gao.gov
Enhancing the management of the U.S. Coast Guard acquisitions	
Public health emergency preparedness	Janet Heinrich, Director Health Care—Public Health Issues (202) 512-7119 henrichj@gao.gov
INS' information technology management weaknesses	Randolph C. Hite, Director Information Technology Architecture and Systems Issues (202) 512-6204 hiter@gao.gov
Building human capital strategies	J.C. Mihm, Director Strategic Issues (202) 512-3236 mihmj@gao.gov
Efforts to combat immigration benefit fraud	Richard M. Stana, Director Tax Administration (202) 512-8777 stanar@gao.gov

Related GAO Products

Homeland Security

Homeland Security: Management Challenges Facing Federal Leadership. [GAO-03-260](#). Washington, D.C.: December 20, 2002.

Highlights of a GAO Forum: Mergers and Transformation: Lessons Learned for a Department of Homeland Security and Other Federal Agencies. [GAO-03-293SP](#). Washington, D.C.: November 14, 2002.

Building Security: Security Responsibilities for Federally Owned and Leased Facilities. [GAO-03-8](#). Washington, D.C.: October 31, 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.

Homeland Security: Information Sharing Activities Face Continued Management Challenges. [GAO-02-1122T](#). Washington, D.C.: October 1, 2002.

Homeland Security: OMB's Temporary Cessation of Information Technology Funding for New Investments. [GAO-03-186T](#). Washington, D.C.: October 1, 2002.

Mass Transit: Challenges in Securing Transit Systems. [GAO-02-1075T](#). Washington, D.C.: September 18, 2002.

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

September 11: Interim Report on the Response of Charities. [GAO-02-1037](#). Washington, D.C.: September 3, 2002.

National Preparedness: Technology and Information Sharing Challenges. [GAO-02-1048R](#). Washington, D.C.: August 30, 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.

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

Review of Studies of the Economic Impact of the September 11, 2001, Terrorist Attacks on the World Trade Center. GAO-02-700R. Washington, D.C.: May 29, 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: A Risk Management Approach Can Guide Preparedness Efforts. [GAO-02-208T](#). Washington, D.C.: October 31, 2001.

Homeland Security: Need to Consider VA's Role in Strengthening Federal Preparedness. [GAO-02-145T](#). Washington, D.C.: October 15, 2001.

Homeland Security: Key Elements of a Risk Management Approach. [GAO-02-150T](#). Washington, D.C.: October 12, 2001.

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

Combating Terrorism

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

Nonproliferation: Strategy Needed to Strengthen Multilateral Export Control Regimes. GAO-03-43. Washington, D.C.: October 25, 2002.

Chemical Weapons: Organization for the Prohibition of Chemical Weapons Needs Comprehensive Plan to Correct Budgeting Weaknesses. GAO-03-5. Washington, D.C.: October 24, 2002.

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

Chemical and Biological Defense: Observations on DOD's Risk Assessment of Defense Capabilities. [GAO-03-137T](#). Washington, D.C.: October 1, 2002.

Chemical Weapons: Lessons Learned Program Generally Effective but Could Be Improved and Expanded. GAO-02-890. Washington, D.C.: September 10, 2002.

Combating Terrorism: Department of State Programs to Combat Terrorism Abroad. GAO-02-1021. Washington, D.C.: September 6, 2002.

Export Controls: Department of Commerce Controls over Transfers of Technology to Foreign Nationals Need Improvement. GAO-02-972. Washington, D.C.: September 6, 2002.

Nonproliferation R&D: NNSA's Program Develops Successful Technologies, but Project Management Can Be Strengthened. GAO-02-904. Washington, D.C.: August 23, 2002.

Diffuse Security Threats: USPS Air Filtration Systems Need More Testing and Cost Benefit Analysis before Implementation. [GAO-02-838](#). Washington, D.C.: August 22, 2002.

Nuclear Nonproliferation: U.S. Efforts to Combat Nuclear Smuggling. GAO-02-989T. Washington, D.C.: July 30, 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.

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

Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness. [GAO-01-162T](#). Washington, D.C.: October 17, 2001.

Combating Terrorism: Selected Challenges and Related Recommendations. [GAO-01-822](#). Washington, D.C.: September 20, 2001.

Combating Terrorism: Actions Needed to Improve DOD's Antiterrorism Program Implementation and Management. [GAO-01-909](#). Washington, D.C.: September 19, 2001.

Combating Terrorism: Comments on H.R. 525 to Create a President's Council on Domestic Preparedness. [GAO-01-555T](#). Washington, D.C.: May 9, 2001.

Combating Terrorism: Observations on Options to Improve the Federal Response. [GAO-01-660T](#). Washington, D.C.: April 24, 2001.

Combating Terrorism: Comments on Counterterrorism Leadership and National Strategy. [GAO-01-556T](#). Washington, D.C.: March 27, 2001.

Combating Terrorism: FEMA Continues to Make Progress in Coordinating Preparedness and Response. [GAO-01-15](#). Washington, D.C.: March 20, 2001.

Combating Terrorism: Federal Response Teams Provide Varied Capabilities; Opportunities Remain to Improve Coordination. [GAO-01-14](#). Washington, D.C.: November 30, 2000.

Combating Terrorism: Issues in Managing Counterterrorist Programs. [GAO/T-NSIAD-00-145](#). Washington, D.C.: April 6, 2000.

Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training. [GAO/NSIAD-00-64](#). Washington, D.C.: March 21, 2000.

Combating Terrorism: Observations on the Threat of Chemical and Biological Terrorism. [GAO/T-NSIAD-00-50](#). Washington, D.C.: October 20, 1999.

Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attack. [GAO/NSIAD-99-163](#). Washington, D.C.: September 7, 1999.

Combating Terrorism: Observations on Growth in Federal Programs. [GAO/T-NSIAD-99-181](#). Washington, D.C.: June 9, 1999.

Combating Terrorism: Analysis of Potential Emergency Response Equipment and Sustainment Costs. [GAO/NSIAD-99-151](#). Washington, D.C.: June 9, 1999.

Combating Terrorism: Use of National Guard Response Teams Is Unclear. [GAO/NSIAD-99-110](#). Washington, D.C.: May 21, 1999.

Combating Terrorism: Issues to Be Resolved to Improve Counterterrorism Operations. [GAO/NSIAD-99-135](#). Washington, D.C.: May 13, 1999.

Combating Terrorism: Observations on Federal Spending to Combat Terrorism. [GAO/T-NSIAD/GGD-99-107](#). Washington, D.C.: March 11, 1999.

Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency. [GAO/NSIAD-99-3](#). Washington, D.C.: November 12, 1998.

Combating Terrorism: Observations on the Nunn-Lugar-Domenici Domestic Preparedness Program. [GAO/T-NSIAD-99-16](#). Washington, D.C.: October 2, 1998.

Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments. [GAO/NSIAD-98-74](#). Washington, D.C.: April 9, 1998.

Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination. [GAO/NSIAD-98-39](#). Washington, D.C.: December 1, 1997.

**Border Security and
Immigration**

Border Security: Implications of 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](#), November 21, 2002.

Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges. [GAO-03-297T](#). Washington, D.C.: November 18, 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.

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

Immigration Enforcement: Challenges to Implementing the INS Interior Enforcement Strategy. [GAO-02-861T](#). Washington, D.C.: June 19, 2002.

Customs Service Modernization: Management Improvements Needed on High-Risk Automated Commercial Environment Project. [GAO-02-545](#). Washington, D.C.: May 13, 2002.

Immigration Benefit Fraud: Focused Approach Is Needed to Address Problems. [GAO-02-66](#). Washington, D.C.: January 31, 2002.

Immigration and Naturalization Service: Overview of Recurring Management Challenges. [GAO-02-168T](#). Washington, D.C.: October 17, 2001.

INS' Southwest Border Strategy: Resource and Impact Issues Remain After Seven Years. [GAO-01-842](#). Washington, D.C.: August 2, 2001.

Immigration Benefits: Several Factors Impede the Timeliness of Application Processing. [GAO-01-488](#). Washington, D.C.: May 4, 2001.

Coast Guard: Actions Needed to Mitigate Deepwater Project Risks. [GAO-01-659T](#). Washington, D.C.: May 3, 2001.

Public Health

Homeland Security: CDC's Oversight of Select Agent Programs. [GAO-03-315R](#). Washington, D.C.: November 22, 2002.

Public Health: Maintaining an Adequate Blood Supply Is Key to Emergency Preparedness. [GAO-02-1095T](#). Washington, D.C.: September 10, 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.

Bioterrorism: The Centers for Disease Control and Prevention's Role in Public Health Protection. [GAO-02-235T](#). Washington, D.C.: November 15, 2001.

Bioterrorism: Review of Public Health and Medical Preparedness. [GAO-02-149T](#). Washington, D.C.: October 10, 2001.

Food Safety and Security: Fundamental Changes Needed to Ensure Safe Food. [GAO-02-47T](#). 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.

Chemical and Biological Defense: Improved Risk Assessments and Inventory Management Are Needed. [GAO-01-667](#). Washington, D.C.: September 28, 2001.

West Nile Virus Outbreak: Lessons for Public Health Preparedness. [GAO/HEHS-00-180](#). Washington, D.C.: September 11, 2000.

Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks. [GAO/NSIAD-99-163](#). Washington, D.C.: September 7, 1999.

Chemical and Biological Defense: Program Planning and Evaluation Should Follow Results Act Framework. [GAO/NSIAD-99-159](#). Washington, D.C.: August 16, 1999.

Combating Terrorism: Observations on Biological Terrorism and Public Health Initiatives. [GAO/T-NSIAD-99-112](#). Washington, D.C.: March 16, 1999.

Aviation Security

Transportation Security Administration: Actions and Plans to Build a Results-Oriented Culture. [GAO-03-190](#). Washington, D.C.: January 13, 2003.

Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System. [GAO-03-344](#). Washington, D.C.: December 20, 2002.

Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenges. [GAO-02-971T](#). Washington, D.C.: July 25, 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 Illustrate Severe Weaknesses in Aviation Security. [GAO-01-1166T](#). Washington, D.C.: September 20, 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: Long-Standing Problems Impair Airport Screeners' Performance. [GAO/RCED-00-75](#). Washington, D.C.: June 28, 2000.

Aviation Security: Slow Progress in Addressing Long-Standing Screener Performance Problems. [GAO/T-RCED-00-125](#). Washington, D.C.: March 16, 2000.

Aviation Security: Progress Being Made, but Long-term Attention Is Needed. [GAO/T-RCED-98-190](#). Washington, D.C.: May 14, 1998.

Aviation Security: FAA's Procurement of Explosives Detection Devices. [GAO/RCED-97-111R](#). Washington, D.C.: May 1, 1997.

Aviation Security: Commercially Available Advanced Explosives Detection Devices. [GAO/RCED-97-119R](#). Washington, D.C.: April 24, 1997.

Aviation Security: Technology's Role in Addressing Vulnerabilities. [GAO/T-RCED/NSIAD-96-262](#). Washington, D.C.: September 19, 1996.

Aviation Security: Urgent Issues Need to Be Addressed. [GAO/T-RCED/NSIAD-96-251](#). Washington, D.C.: September 11, 1996.

Aviation Security: Immediate Action Needed to Improve Security. [GAO/T-RCED/NSIAD-96-237](#). Washington, D.C.: August 1, 1996.

Critical Infrastructure
Protection

Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk. [GAO-03-303T](#). Washington, D.C.: November 19, 2002.

Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed. [GAO-02-781](#). Washington, D.C.: August 30, 2002.

Critical Infrastructure Protection: Significant Challenges Need to Be Addressed. [GAO-02-961T](#). Washington, D.C.: July 24, 2002.

Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach to Protecting Information Systems. [GAO-02-474](#). Washington, D.C.: July 15, 2002.

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

Information Sharing: Practices That Can Benefit Critical Infrastructure Protection. [GAO-02-24](#). Washington, D.C.: October 15, 2001.

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.

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

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities. [GAO-01-1005T](#). Washington, D.C.: July 25, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities. [GAO-01-769T](#). Washington, D.C.: May 22, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities. [GAO-01-323](#). Washington, D.C.: April 25, 2001.

Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination. [GAO/T-AIMD-00-268](#). Washington, D.C.: July 26, 2000.

Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000. [GAO/T-AIMD-00-229](#). Washington, D.C.: June 22, 2000.

Critical Infrastructure Protection: National Plan for Information Systems Protection. [GAO/AIMD-00-90R](#). Washington, D.C.: February 11, 2000.

Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection. [GAO/T-AIMD-00-72](#). Washington, D.C.: February 1, 2000.

Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations. [GAO/T-AIMD-00-7](#). Washington, D.C.: October 6, 1999.

Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences. [GAO/AIMD-00-1](#). Washington, D.C.: October 1, 1999.

Disaster Assistance

September 11: Small Business Assistance Provided in Lower Manhattan in Response to the Terrorist Attacks. [GAO-03-88](#). Washington, D.C.: November 1, 2002.

Disaster Assistance: Improvement Needed in Disaster Declaration Criteria and Eligibility Assurance Procedures. [GAO-01-837](#). Washington, D.C.: August 31, 2001.

Chemical Weapons: FEMA and Army Must Be Proactive in Preparing States for Emergencies. [GAO-01-850](#). Washington, D.C.: August 13, 2001.

Federal Emergency Management Agency: Status of Achieving Key Outcomes and Addressing Major Management Challenges. [GAO-01-832](#). Washington, D.C.: July 9, 2001.

Budget and Management

Human Capital: Effective Use of Flexibilities Can Assist Agencies in Managing Their Workforces. [GAO-03-2](#). Washington, D.C.: December 6, 2002.

Highlights of a GAO Roundtable: The Chief Operating Officer Concept: A Potential Strategy to Address Federal Governance Challenges. [GAO-03-192SP](#). Washington, D.C.: October 4, 2002.

Program Evaluation: Strategies for Assessing How Information Dissemination Contributes to Agency Goals. [GAO-02-923](#). Washington, D.C.: September 30, 2002.

Results-Oriented Cultures: Using Balanced Expectations to Manage Senior Executive Performance. [GAO-02-966](#). Washington, D.C.: September 27, 2002.

Performance Budgeting: Opportunities and Challenges. [GAO-02-1106T](#). Washington, D.C.: September 19, 2002.

Electronic Government: Proposal Addresses Critical Challenges. [GAO-02-1083T](#). Washington, D.C.: September 18, 2002.

Results-Oriented Cultures: Insights for U.S. Agencies from Other Countries' Performance Management Initiatives. [GAO-02-862](#). Washington, D.C.: August 2, 2002.

Acquisition Workforce: Agencies Need to Better Define and Track the Training of Their Employees. [GAO-02-737](#). Washington, D.C.: July 29, 2002.

Managing for Results: Using Strategic Human Capital Management to Drive Transformational Change. [GAO-02-940T](#). Washington, D.C.: July 15, 2002.

U.S. Government Financial Statements: FY 2001 Results Highlight the Continuing Need to Accelerate Federal Financial Management Reform. [GAO-02-599T](#). Washington, D.C.: April 9, 2002.

Coast Guard: Budget and Management Challenges for 2003 and Beyond. [GAO-02-538T](#). Washington, D.C.: March 19, 2002.

Managing for Results: Building on the Momentum for Strategic Human Capital Reform. [GAO-02-528T](#). Washington, D.C.: March 18, 2002.

A Model of Strategic Human Capital Management. [GAO-02-373SP](#). Washington, D.C.: March 15, 2002.

Budget Issues: Long-Term Fiscal Challenges. GAO-02-467T. Washington, D.C.: February 27, 2002.

Managing for Results: Agency Progress in Linking Performance Plans with Budgets and Financial Statements. GAO-02-236. Washington, D.C.: January 4, 2002.

Results-Oriented Budget Practices in Federal Agencies. GAO-01-1084SP. Washington, D.C.: August 2001.

Managing for Results: Federal Managers' Views on Key Management Issues Vary Widely Across Agencies. GAO-01-592. Washington, D.C.: May 2001.

High-Risk Series: An Update. GAO-01-263. Washington, D.C.: January 2001.

Major Management Challenges and Program Risks: A Governmentwide Perspective. GAO-01-241. Washington, D.C.: January 2001.

Major Management Challenges and Program Risks: Department of Transportation. GAO-01-253. Washington, D.C.: January 2001.

Determining Performance and Accountability Challenges and High Risks. GAO-01-159SP. Washington, D.C.: November 2000.

Managing for Results: Using the Results Act to Address Mission Fragmentation and Program Overlap. GAO/AIMD-97-156. Washington, D.C.: August 29, 1997.

Government Restructuring: Identifying Potential Duplication in Federal Missions and Approaches. GAO/T-AIMD-95-161. Washington, D.C.: June 7, 1995.

Reorganization

FBI Reorganization: Initial Steps Encouraging but Broad Transformation Needed. GAO-02-865T. Washington, D.C.: June 21, 2002.

Environmental Protection: Observations on Elevating the Environmental Protection Agency to Cabinet Status. GAO-02-552T. Washington, D.C.: March 21, 2002.

Implementation: The Missing Link in Planning Reorganizations.
[GAO/GGD-81-75](#). Washington, D.C.: March 20, 1981.

Grant Design

Grant Programs: Design Features Shape Flexibility, Accountability, and Performance Information. [GAO/GGD-98-137](#). Washington, D.C.: June 22, 1998.

Federal Grants: Design Improvements Could Help Federal Resources Go Further. [GAO/AIMD-97-7](#). Washington, D.C.: December 18, 1996.

Block Grants: Issues in Designing Accountability Provisions.
[GAO/AIMD-95-226](#). Washington, D.C.: September 1, 1995.

Performance and Accountability and High-Risk Series

Major Management Challenges and Program Risks: A Governmentwide Perspective. [GAO-03-95](#).

Major Management Challenges and Program Risks: Department of Agriculture. [GAO-03-96](#).

Major Management Challenges and Program Risks: Department of Commerce. [GAO-03-97](#).

Major Management Challenges and Program Risks: Department of Defense. [GAO-03-98](#).

Major Management Challenges and Program Risks: Department of Education. [GAO-03-99](#).

Major Management Challenges and Program Risks: Department of Energy. [GAO-03-100](#).

Major Management Challenges and Program Risks: Department of Health and Human Services. [GAO-03-101](#).

Major Management Challenges and Program Risks: Department of Homeland Security. [GAO-03-102](#).

Major Management Challenges and Program Risks: Department of Housing and Urban Development. [GAO-03-103](#).

Major Management Challenges and Program Risks: Department of the Interior. [GAO-03-104](#).

Major Management Challenges and Program Risks: Department of Justice. [GAO-03-105](#).

Major Management Challenges and Program Risks: Department of Labor. [GAO-03-106](#).

Major Management Challenges and Program Risks: Department of State. [GAO-03-107](#).

Major Management Challenges and Program Risks: Department of Transportation. [GAO-03-108](#).

Major Management Challenges and Program Risks: Department of the Treasury. [GAO-03-109](#).

Major Management Challenges and Program Risks: Department of Veterans Affairs. [GAO-03-110](#).

Major Management Challenges and Program Risks: U.S. Agency for International Development. [GAO-03-111](#).

Major Management Challenges and Program Risks: Environmental Protection Agency. [GAO-03-112](#).

Major Management Challenges and Program Risks: Federal Emergency Management Agency. [GAO-03-113](#).

Major Management Challenges and Program Risks: National Aeronautics and Space Administration. [GAO-03-114](#).

Major Management Challenges and Program Risks: Office of Personnel Management. [GAO-03-115](#).

Major Management Challenges and Program Risks: Small Business Administration. [GAO-03-116](#).

Major Management Challenges and Program Risks: Social Security Administration. [GAO-03-117](#).

Major Management Challenges and Program Risks: U.S. Postal Service. [GAO-03-118](#).

High-Risk Series: An Update. [GAO-03-119](#).

High-Risk Series: Strategic Human Capital Management. [GAO-03-120](#).

High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures. [GAO-03-121](#).

High-Risk Series: Federal Real Property. [GAO-03-122](#).

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to GAO Mailing Lists" under "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
 TDD: (202) 512-2537
 Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Official Business
Penalty for Private Use \$300**

Address Service Requested

**Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00**

