United States Government Accountability Office

GAO

Testimony
Before the Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, August 3, 2004

9/11 COMMISSION REPORT

Reorganization, Transformation, and Information Sharing

Statement of the Honorable David M. Walker
Comptroller General of the United States

On 8/4/04 this testimony was reissued because: On page 12, in footnote 11, "OGC" was changed to "OCG" to correct a transposition error. On page 21, in the next to the last sentence in the final paragraph, "might" was changed to "must," and "challenges was changed to "responsibilities and opportunities." In the same pargraph, in the last sentence, " executive" was changed to "effective." These correct transcription errors.

Mr. Chairman and Members of the Committee:

We at GAO applaud the efforts of the 9/11 Commission and the dedicated family members of the victims of that tragic day whose combined efforts have resulted in a definitive account of the past events, and a number of constructive recommendations for the future. The sorrow, loss, anger, and resolve so evident immediately following the September 11, 2001, attacks have been combined in an effort to help assure that our country will never again be caught unprepared. As the Commission notes, we are safer today but we are not safe, and much work remains. Although in today's world we can never be 100 percent secure, and we can never do everything everywhere, we concur with the Commission's conclusion that the American people should expect their government to do its very best.

GAO's mission is to help the Congress improve the performance and ensure the accountability of the federal government for the benefit of the American people. GAO has been actively involved in improving government's performance in the critically important homeland security area both before and after the September 11 attacks. For example, GAO issued over 100 reports on homeland security-related issues and recommended the creation of a national focal point for homeland security before the attacks. We have also been privileged to actively support this Congress and the 9/11 Commission through details of key personnel, testimony before the Congress and the Commission, and sharing our research, products, and experiences.

Just a few days after the tragic events of September 11, I testified about various challenges and strategies to address both our short- and long-term homeland security needs and outlined a framework for addressing our nation's efforts. I emphasized that we as a nation must find the best ways to sustain our efforts over a significant time period, and leverage our finite human, financial, and technological resources in ways that would have the greatest impact. At that time, I identified several key questions that our government needed to address in order to improve the security of the homeland:[1]

1. What are our vision and national objectives to make our homeland more secure?

[1]U.S. General Accounting Office. *Homeland Security: A Framework for Addressing the Nation's Efforts*, GAO-01-1158T (Washington, D.C.: Sept. 21, 2001).

2. What essential elements should constitute the government's strategy for securing the homeland?

3. How should the executive branch and the Congress be organized to address these issues?

4. How should we assess the effectiveness of any homeland security strategy implementation to address the spectrum of threats?

During the past few years, we have seen major efforts to address these questions, such as the formation of the Department of Homeland Security (DHS) and major initiatives such as strengthened passenger and baggage screening, increased border patrols, reform of the Federal Bureau of Investigation (FBI), and the creation of the Northern Command. However, as the 9/11 Commission and our own work indicates, these questions are yet to be fully addressed.

GAO has continued to explore these topics on behalf of this Committee and the Congress, issuing over 200 homeland security related products since the September 11 attacks, developing over 500 recommendations for action, testifying on over 90 occasions before the Congress, and working closely with the Congress and federal agencies, including the FBI, the Department of Defense (DOD), and DHS, to implement key recommendations to improve homeland security mission performance, improve government efficiency, and promote enhanced accountability and oversight to assure the American people that the federal government is doing all that can reasonably be expected.

In your request, you have asked me to address two issues: the lack of effective information sharing and analysis and the need for executive branch reorganization in response to the 9/11 Commission recommendations. Further, you have asked me to address how to remedy problems in information sharing and analysis by transforming the intelligence community from a system of "need to know" to one of a "need to share." The 9/11 Commission has recommended several transformational changes, such as the establishment of a National Counterterrorism Center (NCTC) for joint operational planning and joint intelligence and replacing the current Director of Central Intelligence with a National Intelligence Director (NID) to oversee national intelligence centers across the federal government. The NID would manage the national intelligence program and oversee agencies that contribute to it.

Yesterday, on August 2, 2004, the President asked Congress to create a NID position to be the principal intelligence advisor, appointed by the President, with the advice and consent of the Senate and serving at the pleasure of the President. Unlike the 9/11 Commission, the President did not propose that the NID be within the Executive Office of the President. He also announced that he will establish a NCTC whose Director would report to the NID, and that this center would build upon the analytic work of the existing Terrorist Threat Integration Center. He suggested that a separate center may be necessary for issues of weapons of mass destruction. Finally, he endorsed the 9/11 Commission's call for reorganization of the Congressional oversight structure. There are, however, several substantive differences between the President's proposal and the Commission's recommendations.

While praising the work of the 9/11 Commission, and endorsing several of its major recommendations in concept, the President differed with the Commission on certain issues. These differences reflect that reasoned and reasonable individuals may differ, and that several methods may exist to effectuate the transformational changes recommended. However, certain common principles and factors outlined in my statement today should help guide the debate ahead.

Although the creation of a NID and a NCTC would be major changes for the intelligence community, other structural and management changes have occurred and are continuing to occur in government that provide lessons for the intelligence community transformation. While the intelligence community has historically been addressed separately from the remainder of the federal government, and while it undoubtedly performs some unique missions that present unique issues (e.g., the protection of sources and methods) its major transformational challenges in large measure are the same as those that face most government agencies.

As a result, GAO's findings, recommendations, and experience in reshaping the federal government to meet Twenty-First Century challenges will be directly relevant to the intelligence community and the recommendations proposed by the 9/11 Commission. Reorganizing government can be an immensely complex activity with both opportunities and risks. As a result, those who propose to reorganize government must make their rationale clear and build a consensus for change if proposed reorganizations are to succeed and be sustained. All key players must be involved in the process.

The goal of improving information sharing and analysis with a focus upon the needs of the consumers of such improved information for specific types of threats can provide one of the powerful guiding principles necessary for successful transformation. The elevated threat advisory (orange alert) issued this past weekend for certain financial institutions in particular regions dramatically illustrates the value of improved analysis and sharing of information specific enough to guide effective and efficient preparedness actions by those most at risk. Earlier threat advisories issued by DHS were criticized for lack of specificity, "one size fits all" applicability, and lack of "actionable" information.

In my testimony today, I will cover four major points. First, I describe the rationale for improving effective information sharing and analysis, and suggest some ways to achieve positive results. Improvements would include, for example, developing a comprehensive and coordinated national plan to facilitate information sharing and relationships. Second, I provide some overview perspectives on reorganizational approaches to improve performance and note necessary cautions. For example, the Congress has an important role to play in the design and implementation of a new structure, and oversight will be key to success. Third, I illustrate that strategic human capital management must be the centerpiece of any serious change management initiative or any effort to transform the cultures of government agencies, including that of the intelligence community. Strategic management includes, for example, consideration of human capital flexibilities. Finally, I emphasize the importance of results-oriented strategic planning and implementation for the intelligence arena, focusing management attention on outcomes, not outputs, and the need for effective accountability and oversight to maintain focus upon improving performance. For example, much more attention needs to be paid to defining goals and measures, and providing for increased oversight of the performance of the intelligence community. I conclude by applying these concepts and principles to the challenges of reform in the intelligence community.

This testimony draws upon our wide-ranging, completed, and ongoing work, and our institutional knowledge on homeland security, combating terrorism, and various government organizational and management issues. We conducted our work in accordance with generally accepted government auditing standards.

Stronger Intelligence Sharing Is Needed

Mr. Chairman, there is a continuing and heightened need for better and more effective and comprehensive information sharing. We agree the intelligence community needs to move from a culture of "need to know" to "need to share." The 9/11 Commission has made observations regarding information sharing, and recommended procedures to provide incentives for sharing and creating a "trusted information network." Many Commission recommendations address the need to improve information and intelligence collection, sharing, and analysis within the intelligence community itself. In addition, we must not lose sight of the fact that the purpose of improving information analysis and sharing is to provide better information throughout the federal government, and ultimately also to state and local governments, the private sector, and our citizens, so that collectively we are all better prepared. I want to make it clear that such information sharing must protect confidential sources and methods, and we do not propose any changes that would infringe upon those protections.

In addition, as the Congress considers the Commission's recommendations, I would also recommend that it consider the role that state and local agencies and the private sector should play as informed partners in homeland security. The Commission's work, as is the case with our own observations, notes the changing perspective of "federal" versus "other entities'" roles in homeland security and homeland defense. In performing its constitutional role of providing for the common defense, we have observed that the federal government must prevent and deter terrorist attacks on our homeland as well as detect impending danger before attacks occurs. Although it may be impossible to detect, prevent, or deter every attack, steps can and must be taken to reduce the risk posed by the threats to homeland security. Furthermore, in order to be successful in this area, the federal government must partner with a variety of organizations, both domestic and international.

Traditionally, protecting the homeland against threats was generally considered a federal responsibility. To meet this responsibility, the federal government (within and across federal agencies) gathers intelligence, which is often classified as national security information. This information is protected and safeguarded to prevent unauthorized access by requiring appropriate security clearances and a "need to know." Normally, the federal government did not share national-level intelligence with states and cities, since they were not viewed as having a significant role in preventing terrorism. Therefore, the federal government did not generally grant state and city officials access to classified information. After the September 11 attacks, however, the view that states and cities do not have

a significant role in homeland security changed, and the "need to share" intelligence information became clear.[2]

However, reconciling the need to share with actually sharing has been at the heart of the 9/11 Commission's recommendations and our own findings and observations on practices to improve information sharing. In work begun before the September 11 attacks,[3] we reported on information-sharing practices of organizations that successfully share sensitive or time-critical information. We found that these practices include:

- establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents,
- developing standards and agreements on how shared information will be used and protected,
- establishing effective and appropriately secure communications mechanisms, and
- taking steps to ensure that sensitive information is not inappropriately disseminated.

As you might recall, we also testified before this committee last year on information sharing. GAO has made numerous recommendations related to sharing, particularly as they relate to fulfilling DHS's critical infrastructure protection responsibilities.[4] The Homeland Security Information Sharing Act, included in the Homeland Security Act of 2002 (P.L. 107-296), requires the President to prescribe and implement procedures for facilitating homeland security information sharing and establishes authorities to share different types of information, such as grand jury information; electronic, wire, and oral interception information; and foreign intelligence information. In July 2003, the President assigned

[2]U.S. General Accounting Office, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760 (Washington, D.C.: August 2003).

[3]U.S. General Accounting Office, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

[4]U.S. General Accounting Office. *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-1165T (Washington, D.C.: Sept. 17, 2003); GAO-03-715T (May 8, 2003).

these functions to the Secretary of Homeland Security, but no deadline was established for developing such information sharing procedures..

To accomplish its missions, DHS must gain access to, receive, and analyze law enforcement information, intelligence information, and other threat, incident, and vulnerability information from federal and nonfederal sources, and it must analyze such information to identify and assess the nature and scope of terrorist threats. DHS must also share information both internally and externally with agencies and law enforcement on such things as goods and passengers inbound to the United States and individuals who are known or suspected terrorists and criminals (e.g., watch lists).

As we reported in June 2002,[5] the federal government had made progress in developing a framework to support a more unified effort to secure the homeland, including information sharing. However, this work found additional needs and opportunities to enhance the effectiveness of information sharing among federal agencies with homeland security or homeland defense responsibilities, and with various state and city law enforcement agencies that have a key role in homeland security, as well as with the private sector.

As we reported in August 2003,[6] efforts to improve intelligence and information sharing still needed to be strengthened. Intelligence- and information- sharing initiatives implemented by states and cities were not effectively coordinated with those of federal agencies, nor were they coordinated within and between federal entities. Furthermore, neither federal, state, nor city governments considered the information-sharing process to be effective. For example, information on threats, methods, and techniques of terrorists was not routinely shared; information that was shared was not perceived as timely, accurate, or relevant; and federal officials have not established comprehensive processes or procedures to promote effective information sharing. At that time, we recommended that the Secretary of Homeland Security work with the heads of other federal agencies and state and local authorities to:

[5]U.S. General Accounting Office, *Homeland Security: Key Elements to Unify Efforts Are Under Way but Uncertainty Remains*, GAO-02-610 (Washington, D.C.: June 7, 2002).

[6]GAO-03-760.

- incorporate the existing information-sharing guidance that is contained in the various national strategies and information-sharing procedures required by the Homeland Security Act,

- establish a clearinghouse to coordinate the various information-sharing initiatives to eliminate possible confusion and duplication of effort,

- fully integrate states and cities into the national policy-making process for information sharing and take steps to provide greater assurance that actions at all levels of government are mutually reinforcing,

- identify and address the perceived barriers to federal information sharing, and

- use a survey method or a related data collection approach to determine, over time, the needs of private and public organizations for information related to homeland security and to measure progress in improving information sharing at all levels of government.

DHS concurred with the above recommendations.

DHS and other federal agencies have instituted major counterterrorism efforts involving information and intelligence sharing over the past 2 years. For example, the Terrorist Threat Integration Center (T-TIC) was designed to improve the collection, analysis, and sharing of all counterterrorism intelligence gathered in the United States and overseas. The DHS Information Analysis and Infrastructure Protection (IAIP) Directorate is intended to receive intelligence from a variety of federal sources and act as a central fusion point for all intelligence relevant to homeland security and related critical infrastructure protection. Furthermore, the FBI has created a new Office of Intelligence, established a National Joint Terrorism Taskforce, expanded its Joint Terrorist Task Forces (JTTFs), and recently made operational an interagency joint Terrorist Screening Center.

Although improvements had been made, we continue to identify needs, such as developing a comprehensive and coordinated national plan to facilitate information-sharing on critical infrastructure protection (CIP); developing productive information sharing relationships among the federal government and state and local governments and the private sector; and providing appropriate incentives for nonfederal entities to increase information sharing with the federal government and enhance other critical infrastructure protection efforts. As we recently reported,

information sharing and analysis centers (ISACs) have identified a number of challenges to effective CIP information sharing between the federal government and state and local governments and the private sector, including sharing information on physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices. Such challenges include building trusted relationships; developing processes to facilitate information sharing; overcoming barriers to information sharing; clarifying the roles and responsibilities of the various government and private sector entities that are involved in protecting critical infrastructure; and funding ISAC operations and activities.[7]

Although DHS has taken a number of actions to implement the public/private partnership called for by federal CIP policy, it has not yet developed a plan that describes how it will carry out its information-sharing responsibilities and relationships, including consideration of appropriate incentives for nonfederal entities to increase information sharing with the federal government, increase sector participation, and perform other specific tasks to protect the critical infrastructure. Such a plan could encourage improved information sharing among the ISACs, other CIP entities, and the department by clarifying the roles and responsibilities of all the entities involved and clearly articulating actions to address the challenges that remain.

The department also lacks policies and procedures to ensure effective coordination and sharing of ISAC-provided information among the appropriate components within the department. Developing such policies and procedures would help ensure that information is appropriately shared among its components and with other government and private sector CIP entities. GAO recommended that the Secretary of Homeland Security direct officials within DHS to (1) proceed with the development of an information-sharing plan that describes the roles and responsibilities of DHS, the ISACs, and other entities and (2) establish appropriate department policies and procedures for interactions with other CIP entities and for coordination and information sharing among DHS components. DHS has generally agreed with our findings and recommendations.

[7]U.S. General Accounting Office. *Critical Infrastructure Protection*: *Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, D.C.: July 9, 2004).

DHS has also implemented the Homeland Security Advisory System. Utilizing five color-coded threat levels, the system was established in March 2002 to disseminate information regarding the risk of terrorist acts to federal agencies, states and localities, and the public. Our recent work indicates that DHS has not yet officially documented communication protocols for providing threat information and guidance to federal agencies and states, with the result that some federal agencies and states may first learn about changes in the national threat level from media sources. Moreover, federal agencies and states responding to our inquiries indicated that they generally did not receive specific threat information and guidance, and they believed this shortcoming hindered their ability to determine whether they were at risk as well as their ability to determine and implement appropriate protective measures.[8]

In addition, there is a need for an improved security clearance process so that state, local, and private sector officials have the access to information they need, but with appropriate security safeguards in place, while efforts to improve information sharing continue. In a recent report,[9] we described the FBI's process for granting access to classified information for state and local law enforcement officials. The FBI's goal is to complete the processing for secret security clearances within 45 to 60 days and top secret security clearances within 6 to 9 months. While the FBI's processing of top secret security clearances has been generally timely, that was not the case for secret clearances. However, the FBI made substantial improvements in 2003 to the timeliness of processing secret clearances.

We also have conducted a body of work that has found that long-standing security clearance backlogs and delays in determining clearance eligibility affect industry personnel, military members, and federal employees. For example, as we reported in May of this year,[10] more than 187,000 reinvestigations, new investigations, or clearance adjudications were not completed for industry personnel alone within established time frames.

[8]U.S. General Accounting Office, *Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System*, GAO-04-682 (Washington, D.C.: June 25, 2004).

[9]U.S. General Accounting Office. *Security Clearances: FBI Has Enhanced Its Process for State and Local Law Enforcement Officials*, GAO-04-596 (Washington, D.C.: April 30, 2004).

[10]U.S. General Accounting Office, *DOD Personnel Clearances: Additional Steps Can Be Taken to Reduce Backlogs and Delays in Determining Security Clearance Eligibility for Industry Personnel*, GAO-04-632 (Washington, D.C: May 26, 2004).

Delays in conducting investigations and determining clearance eligibility can increase national security risks, prevent industry personnel from beginning or continuing work on classified programs and activities, or otherwise hinder the sharing of classified threat information with officials having homeland security or homeland defense responsibilities.

The FBI has also taken a number of steps to enhance its information sharing with state and local law enforcement officials, such as providing guidance and additional staffing. The FBI has further increased the number of its JTTFs, increasing them from 35 prior to the September 11 attacks to 84 as of July 2004 and state and local law enforcement officials' participation on these task forces has been increased. The FBI has at least one JTTF in each of its 56 field locations and plans to expand to 100. The FBI also circulates declassified intelligence through a weekly bulletin and provides threat information to state and local law enforcement officials via various database networks.

These critical needs for better information and information sharing identified by federal, state, and local governments and the private sector must form the clear rationale and basis for transformation of the intelligence community. Reorganization isn't the objective; rather it is improving government performance to meet twenty first century information sharing requirements. 9/11 Commission Chairman Thomas H. Kean and Vice-Chairman Lee H. Hamilton, in their testimony before the Senate Governmental Affairs Committee on July 30, 2004, noted:

"There is a fascination in Washington with bureaucratic solutions—rearranging the wiring diagrams, creating new organizations. We do recommend some important institutional changes. We will articulate and defend those proposals. But we believe reorganizing governmental institutions is only a part of the agenda before us. Some of the saddest aspects of the 9/11 story are the outstanding efforts of so many individual officials straining, often without success, against the boundaries of the possible. Good people can overcome bad structures. They should not have to. We have the resources and the people. We need to combine them more effectively, to achieve unity of effort."

GAO agrees with this comment, and we have noted several related suggestions below.

While Changes May be Needed, Caution and Care Must be Taken

As the committee is aware, GAO has done extensive work on federal organizational structure and how reorganization can improve performance. The 9/11 Commission has recommended major changes to unify strategic intelligence and operational planning with a National Counterterrorism Center and provide the intelligence community with a new National Intelligence Director. As the Congress and the administration consider the 9/11 Commission's recommendations, they should consider how best to address organizational changes, roles and responsibilities, and functions for intelligence-sharing effectiveness.

In response to the emerging trends and long-term fiscal challenges the government faces in the coming years, we have an opportunity to create highly effective, performance-based organizations that can strengthen the nation's ability to meet the challenges of the twenty first century and reach beyond our current level of achievement. The federal government cannot accept the status quo as a given—we need to reexamine the base of government policies, programs, structures, and operations. We need to minimize the number of layers and silos in government, emphasize horizontal versus vertical actions, while moving our policy focus to coordination and integration. The result, we believe, will be a government that is effective and relevant to a changing society—a government that is as free as possible of outmoded commitments and operations that can inappropriately encumber the future, reduce our fiscal flexibility, and prevent future generations from being able to make choices regarding what roles they think government should play.

Many departments and agencies, including those of the intelligence community, were created in a different time and in response to challenges, threats, and priorities very different from today's world. Some have achieved their one time missions and yet they are still in business. Many have accumulated responsibilities beyond their original purposes. Many are still focused on their original mission that may not be relevant or as high a priority in today's world. Others have not been able to demonstrate how they are making a difference in real and concrete terms. Still others have overlapping or conflicting roles and responsibilities. Redundant, unfocused, uncoordinated, outdated, misaligned, and nonintegrated programs and activities waste scarce funds, confuse and frustrate program customers, and limit overall efficiency and effectiveness.[11] These are the

[11]U.S. General Accounting Office, *Managing in the New Millennium: Shaping a More Efficient and Effective Government for the 21st Century*, GAO/T-OCG-00-9 (Washington, D.C.: Mar. 29, 2000).

charges highlighted by the 9/11 Commission's findings and recommendations.

The problems the 9/11 Commission has described with our intelligence activities indicate a strong need for reexamining the organization and execution of those activities. However, any restructuring proposal requires careful consideration. Fixing the wrong problems or even worse, fixing the right problems poorly, could cause more harm than good.

Past executive reorganization authority has served as an effective tool for achieving fundamental reorganization of federal operations. As I have testified before this committee,[12] the granting of executive reorganization authority to the President can serve to better enable the President to propose government designs that would be more efficient and effective in meeting existing and emerging challenges involving the intelligence community and information sharing with other entities. However, lessons learned from prior federal reorganization efforts suggest that reorganizing government can be an immensely complex activity that requires consensus on both the goals to be achieved and the process for achieving them. Prior reorganization authority has reflected a changing balance between legislative and executive roles. Periodically, between 1932 and 1984, the Congress passed legislation providing the President one form or another of expedited reorganization authority.[13]

Congressional involvement is needed not just in the initial design of the reorganization, but in what can turn out to be a lengthy period of implementation. The Congress has an important role to play—in both its legislative and oversight capacities—in establishing, monitoring, and maintaining progress to attain the goals envisioned by government transformation and reorganization efforts. However, as the 9/11 Commission has noted, past oversight efforts in the intelligence area have been wholly inadequate.

To ensure efficient and effective implementation and oversight, the Congress will also need to consider realigning its own structure. With

[12]U.S. General Accounting Office, *Executive Reorganization Authority: Balancing Executive and Congressional Roles in Shaping the Federal Government's Structure*, GAO-03-624T (Washington, D.C.: April 3, 2003).

[13]Ronald C. Moe, Congressional Research Service, *The President's Reorganization Authority: Review and Analysis* (Washington, D.C.: Mar. 8, 2001).

changes in the executive branch, the Congress should adapt its own organization. For example, the Congress has undertaken a reexamination of its committee structure, with the implementation of DHS. The DHS legislation instructed both houses of Congress to review their committee structures in light of the reorganization of homeland security responsibilities within the executive branch. Similarly, the 9/11 Commission recommends realigning congressional oversight to support its proposals to reorganize intelligence programs.

Addressing Intelligence Human Capital Needs Requires Strategic Management

The 9/11 Commission stresses the need for stronger capabilities and expertise in intelligence and national security to support homeland security. For example, the Commission recommends rebuilding the Central Intelligence Agency's analytical capabilities, enhancing the agency's human intelligence capabilities, and developing a stronger language program.

We believe, Mr. Chairman, that at the center of any serious change management initiative are the people involved—people define the organization's culture, drive its performance, and embody its knowledge base. They are the source of all knowledge, process improvement, and technological enhancement efforts. As such, strategic human capital (or people) strategy is the critical element to maximizing government's performance and ensuring accountability of our intelligence community and homeland security efforts.

Experience shows that failure to adequately address—and often even consider—a wide variety of people and cultural issues is at the heart of unsuccessful organizational transformations. Recognizing the "people" element in these initiatives and implementing strategies to help individuals maximize their full potential in the new environment is the key to a successful transformation of the intelligence community and related homeland security organizations. Thus, organizational transformations that incorporate strategic human capital management approaches will help to sustain agency efforts and improve the efficiency, effectiveness, and accountability of the federal government. To help, we have identified a

set of practices that have been found to be central to any successful transformation effort.[14]

Committed, sustained, highly qualified, and inspired leadership, and persistent attention by all key parties in the successful implementation of organizational transformations, will be essential, if lasting changes are to be made and the challenges we are discussing today are to be effectively addressed. It is clear that in a knowledge-based federal government, including the intelligence community, people—human capital—are the most valuable asset. How these people are organized, incented, enabled, empowered, and managed is key to the reform of the intelligence community and other organizations involved with homeland security.

We have testified that federal human capital strategies are not yet appropriately constituted to meet current and emerging challenges or to drive the needed transformation across the federal government. The basic problem has been the long-standing lack of a consistent approach to marshaling, managing, and maintaining the human capital needed to maximize government performance and ensure its accountability to the people. Thus, federal agencies involved with the intelligence community and other homeland security organizations will need the most effective human capital systems to address these challenges and succeed in their transformation efforts during a period of sustained budget constraints. This includes aligning their strategic planning and key institutional performance with unit and individual performance management and reward systems.

Fortunately, the Congress has passed legislation providing many of the authorities and tools agencies need. In fact, more progress in addressing human capital challenges was made in the last 3 years than in the last 20, and significant changes in how the federal workforce is managed are under way. For example, the Congress passed legislation providing governmentwide human capital flexibilities, such as direct hire authority, the ability to use category rating in the hiring of applicants instead of the "rule of three," and the creation of chief human capital officer (CHCO) positions and the CHCO Council. In addition, individual agencies—such as the National Aeronautical and Space Administration (NASA), DoD, and

[14]U. S. General Accounting Office, *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, GAO-03-669 (Washington, D.C.: July 2, 2003).

DHS—received flexibilities intended to help them manage their human capital strategically to achieve results.

While many agencies have received additional human capital flexibilities, additional ones may be both needed and appropriate for the intelligence, homeland security, national defense, and selected other agencies. While the above authorities are helpful, in order to enable agencies to rapidly meet their critical human capital needs, the Congress should consider legislation granting selected agency heads the authority to hire a limited number of positions for a stated period of time (e.g., up to 3 years) on a noncompetitive basis. The Congress has passed legislation granting this authority to the Comptroller General of the United States and it has helped GAO to address a range of critical needs in a timely, effective, and prudent manner over many years.

Recent human capital actions have significant precedent-setting implications for the rest of government. They represent progress and opportunities, but also present legitimate concerns. We are fast approaching the point where "standard governmentwide" human capital policies and processes are neither standard nor governmentwide. As the Congress considers the need for additional human capital authorities for the intelligence community, it should keep in mind that human capital reform should avoid further fragmentation within the civil service, ensure reasonable consistency within the overall civilian workforce, and help maintain a reasonably level playing field among federal agencies in competing for talent. Importantly, this is not to delay needed reforms for any agency, but to accelerate reform across the federal government and incorporate appropriate principles and safeguards.

As the Congress considers reforms to the intelligence communities' human capital policies and practices, it should require that agencies have in place the institutional infrastructure needed to make effective use of any new tools and authorities. At a minimum, this institutional infrastructure includes a human capital planning process that integrates the agency's human capital policies, strategies, and programs with its program goals and mission and desired outcomes; the capabilities to effectively develop and implement a new human capital system; and, importantly, a set of appropriate principles and safeguards, including reasonable transparency and appropriate accountability mechanisms, to ensure the fair, effective, credible, nondiscriminatory implementation and application of a new system.

Managing for Results

As Chairman Kean and Vice-Chairman Hamilton caution, organizational changes are just a part of the reforms needed. The Commission rightly says that effective public policies need concrete objectives, agencies need to be able to measure success, and the American people are entitled to see some standards for performance so they can judge, with the help of their elected representatives, whether the objectives are being met. To comprehensively transform government to improve intelligence and homeland security efforts, we must also carefully assess and define mission needs, current capabilities, resource practicalities, and priorities. And we must implement our plans to achieve those mission needs.

The federal government is well short of where it needs to be in setting national homeland security goals, including those for intelligence and other mission areas, to focus on results—outcomes—not inputs and outputs which were so long a feature of much of the federal government's strategic planning. We are concerned that the tenets of results management—shifting management attention from inputs, processes, and outputs to what is accomplished with them (outcomes or results)—still are elusive in homeland security goal setting and operational planning. We advocate a clear and comprehensive focus on homeland security results management, including the mission of intelligence and information sharing. Results management should have the elements to determine (1) if homeland security results are being achieved within planned timeframes, (2) if investments and resources are being managed properly, (3) if results are being integrated into ongoing decision making and priority setting, and (4) what action is needed to guide future investment policies and influence behavior to achieve results. These actions go far beyond a limited focus on organizational structure.

As the Gilmore Commission stated, a continuing problem for homeland security has been the lack of clear strategic guidance from the federal level about the definition and objectives of preparedness and how states and localities will be evaluated in meeting those objectives.[15] The 9/11 Commission's broad recommendations, if adopted, will require a thoughtful, detailed, results-oriented management approach in defining specific goals, activities, and resource requirements.

[15]The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *V. Forging America's New Normalcy*, (Arlington, VA.: Dec. 15, 2003).

The track record for homeland security results management to date is spotty. The *National Strategy for Homeland Security*, issued by the administration in July 2002, was intended to mobilize and organize the nation to secure the homeland from terrorist attacks.[16] Intelligence and warning was one of its critical mission areas. Despite the changes over the past two years, the National Strategy has not been updated. In general, initiatives identified in the strategy do not provide a baseline set of performance goals and measures upon which to assess and improve preparedness, stressing activities rather than results. For example, for intelligence and warning, the National Strategy identified major initiatives that are activities, such as implementing the Homeland Security Advisory System, utilizing dual-use analysis to prevent attacks; and employing "red team" techniques.

Establishing clear goals and performance measures is critical to ensuring both a successful and a fiscally responsible and sustainable preparedness effort. We are currently doing work on the extent to which the National Strategy's goals are being implemented by federal agencies. Senator Lieberman has recently introduced legislation requiring executive branch efforts to produce a national homeland security strategy. We support the concept of a legislatively required strategy that can be sustained across administrations and provides a framework for congressional oversight. Before the administration's National Strategy for Homeland Security was issued, we had stated that the strategy should include steps designed to (a) reduce our vulnerability to threats; (b) use intelligence assets and other broad-based information sources to identify threats and share information as appropriate; (c) stop incidents before they occur; (d) manage the consequences of an incident; and (e) in the case of terrorist attacks, respond by all means available, including economic, diplomatic, and military actions that, when appropriate, are coordinated with other nations.[17] Earlier this year we provided a set of desirable characteristics for any effective national strategy that could better focus national

[16]The White House, *The National Strategy for Homeland Security*, (Washington, D.C.: July 2002).

[17]U.S. General Accounting Office, *Homeland Security: Challenges and Strategies in Addressing Short- and Long-Term National Needs*, GAO-02-160T (Washington, D.C.: Nov. 7, 2001).

homeland security decision making and increase the emphasis on outcomes.[18]

Strategic planning is critical to provide mission clarity, establish long-term performance strategies and goals, direct resource decisions, and guide transformation efforts. In this context, we are reviewing the DHS strategic planning efforts. Our work includes a review of the manner by which the Department's planning efforts support the National Strategy for Homeland Security and the extent to which its strategic plan reflects the requirements of the Government Performance and Results Act of 1993.

DHS's planning efforts are evolving. The current published DHS strategic plan contains vague strategic goals and objectives for all its mission areas, including intelligence, and little specific information to guide congressional decision making. For example, the strategic plan includes an overall goal to identify and understand threats, assess vulnerabilities, determine potential impacts, and disseminate timely information to DHS's homeland security partners and the American public. That goal has very general objectives, such as gathering and fusing all terrorism-related intelligence and analyzing and coordinating access to information related to potential terrorist or other threats. Discussion of annual goals are missing, and supporting descriptions of means and strategies are vague, making it difficult to determine if they are sufficient to achieve the objectives and overall goals. These and related issues will need to be addressed as the DHS planning effort moves forward.

In another effort to set expectations, the President, through Homeland Security Presidential Directive 8,[19] has tasked the Department of Homeland Security with establishing measurable readiness priorities and targets appropriately balancing the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies with resources required to prevent, respond to, and recover from them. The task also is to include readiness metrics and elements supporting the national preparedness goal, including standards for preparedness assessments and strategies, and a system for assessing the nation's overall preparedness to respond to major

[18]U.S. General Accounting Office, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[19]The White House, *Homeland Security Presidential Directive 8 (National Preparedness)*, (Washington, D.C.: Dec. 17, 2003).

events, especially involving acts of terrorism. However, those taskings have yet to be completed, but they will have to address the following questions:

- What are the appropriate national preparedness goals and measures? What are appropriate subgoals for specific areas such as critical infrastructure sectors?

- Do these goals and subgoals take into account other national goals such as economic security or the priority objectives of the private sector or other levels of government?

- Who should be accountable for achieving the national goals and subgoals?

- How would a national results management and measurement system be crafted, implemented, and sustained for the national preparedness goals?

- How would such a system affect needs assessment and be integrated with funding and budgeting processes across the many organizations involved in homeland security?

However, even if we have a robust and viable national strategy for homeland security, DHS strategic plan, and national preparedness goals, the issue of implementation remains. Implementation cannot be assured, or corrective action taken, if we are not getting the results we want, without effective accountability and oversight. The focus for homeland security must be on constantly staying ready and prepared for unknown threats and paying attention to improving performance. In addition to continuing our ongoing work in major homeland security mission areas such as border and transportation security and emergency preparedness, GAO can help the Congress more effectively oversee the intelligence community, and any changes should consider, in our view, an appropriate role for the GAO.

With some exceptions, GAO has broad-based authority to conduct reviews relating to various intelligence agencies. However, because of historical resistance from the intelligence agencies and the general lack of support from the intelligence committees in the Congress, GAO has done limited work in this community over the past 25 years. For example, within the past 2 years, we have done a considerable amount of work in connection with the FBI and its related transformational efforts. In addition, GAO has

recently had some interaction with the Defense Intelligence Agency in connection with its transformation efforts. Furthermore, GAO has conducted extensive work on a wide range of government transformational and homeland security issues over the past several years. As always, we stand ready to offer GAO's assistance in support of any of the Congress' oversight needs.

The Challenges Faced in Intelligence Reform

In conclusion, on the basis of GAO's work in both the public and the private sector over many years, and my own change management experience, it is clear to me that many of the challenges that the intelligence community faces are similar or identical to the transformation challenges applicable to many other federal agencies, including GAO. Specifically, while the intelligence agencies are in a different line of business than other federal agencies, they face the same challenges when it comes to strategic planning and budgeting, organizational alignment, human capital strategy, and the management of information technology, finances, knowledge, and change.

For the intelligence community, effectively addressing these basic business transformation challenges will require action relating to five key dimensions, namely, structure, people, process, technology, and partnerships. It will also require a rethinking and cultural transformation in connection with intelligence activities both in the executive branch and in the Congress.

With regard to the structure dimension, there are many organizational units within the executive branch and in the Congress with responsibilities in the intelligence and homeland security areas. Basic organizational and management principles dictate that, absent a clear and compelling need for competition or checks and balances, there is a need to minimize the number of entities and levels in key decision making, oversight, and other related activities. In addition, irrespective of how many units and levels are involved, someone has to be in charge of all key planning, budgeting, and operational activities. One person should be responsible and accountable for all key intelligence activities within the executive branch, and that person should report directly to the President. This position must also have substantive strategic planning, budget, operational integration, and accountability responsibilities and opportunities for the intelligence community in order to be effective. In addition, this person should be appointed by the President and confirmed by the Senate in order to help facilitate success and ensure effective oversight.

With regard to the oversight structure of the Congress, the 9/11 Commission noted that there are numerous players involved in intelligence activities and yet not enough effective oversight is being done. As a result, a restructuring of intelligence and homeland security related activities in the Congress is also needed. In this regard, it may make sense to separate responsibility for intelligence activities from personal privacy and individual liberty issues in order to ensure that needed attention is given to both while providing for a check and balance between these competing interests.

With regard to the people dimension, any entity is only as good as its people, and as I stated earlier, the intelligence community is no exception. In fact, since the intelligence community is in the knowledge business, people are of vital importance. The people challenge starts at the top, and key leaders must be both effective and respected. In addition, they need to stay in their positions long enough to make a real and lasting difference. In this regard, while the FBI director has a 10-year term appointment, most agency heads serve at the pleasure of their appointing official and may serve a few years in their respective positions. This is a problem when the agency is in the need of a cultural transformation, such as that required in the intelligence community, which typically takes at least 5 to 7 years to effectuate.

In addition to having the right people and the right "tone at the top," agencies need to develop and execute workforce strategies and plans helping to ensure that they have the right people with the right skills in the required numbers to accomplish their missions. Many of these missions have changed in the post-Cold War and post September 11 world. This is especially critical in connection with certain skills that are in short supply, such as information technology and certain languages, such as Arabic. In addition, as the 9/11 Commission and others have noted, it is clear that additional steps are necessary to strengthen our human intelligence capabilities.

With regard to the process and technology dimensions, steps need to be taken to streamline and expedite the processes used to analyze and disseminate the tremendous amount of intelligence and other information available to the intelligence community. This will require extensive use of technology to sort and distribute information both within agencies and between agencies and other key players in various sectors both domestically and internationally, as appropriate. The 9/11 Commission and others have noted various deficiencies in this area, such as the FBI's information technology development and implementation challenges. At

the same time, some successes have occurred during the past 2 years that address process and technology concerns. For example, the Terrorist Screening Center, created under Homeland Security Presidential Directive 6 is intended to help in the consolidation of the federal government's approach to terrorism screening.[20] This center has taken a number of steps to address various organizational, technological, integration, and other challenges, and it may serve as a model for other needed intra- and interorganizational efforts.

With regard to partnerships, it has always been difficult to create an environment of shared responsibility, shared resources, and shared accountability for achieving difficult missions. Effective partnerships require a shared vision, shared goals, and shared trust in meeting agreed-upon responsibilities. Partnerships also mean that power is shared. Too often we have seen both public and private sector organizations where the term "partnership" is often voiced, but the reality is more a jockeying for dominance or control over the "partner." The end result is that resources are not shared, the shared mission is never complete or adequate, and opportunities for true strategic alliance are squandered. In the intelligence arena, we know the potential end result is failure for the nation.

With regard to the cultural dimension, this is both the softest and the hardest to deal with. By the softest, I mean it involves the attitudes and actions of people and entities. By the hardest, I mean that changing long-standing cultures can be a huge challenge, especially if the efforts involve organizational changes in order to streamline, integrate, and improve related capabilities and abilities. This includes both execution and oversight-related activities. As the 9/11 Commission and others have noted, such a restructuring is needed in both the executive branch and the Congress. This will involve taking on the vested interests of many powerful players, and as a result, it will not be easy, but it may be essential, especially if we expect to go from a "need to know" to a "need to share' approach. As I have often said, addressing such issues takes patience, persistence, perspective, and pain before you prevail. Such is the case with many agency transformational efforts, including those within our own GAO. However, given the challenges and dangers that we face in the post 9/11 world, we cannot afford to wait much longer. The time for action is now.

[20]The White House, *Homeland Security Presidential Directive-6* (Integration and Use of Screening Information), Washington, D.C.: Sept. 16, 2003.

Conclusion

Mr. Chairman, in its final report, the Gilmore Commission stated:

"There will never be an end point in America's readiness. Enemies will change tactics, citizens' attitudes about what adjustments in their lives they will be willing to accept will evolve and leaders will be confronted with legitimate competing priorities that will demand attention….In the end, America's response to the threat of terrorism will be measured by how we manage risk. There will never be a 100% guarantee of security for our people, the economy, and our society. We must resist the urge to seek total security—it is not achievable and drains our attention from those things that can be accomplished."[21]

Managing risk is not simply about putting new organizations in place. It requires us to think about what must be protected, define an acceptable level of risk, and target limited resources while keeping in mind that the related costs must be affordable and sustainable. Perhaps more important, managing risk requires us to constantly operate under conditions of uncertainty, where foresight, anticipation, responsiveness, and radical adaptation are vital capabilities.

We can and we must enhance and integrate our intelligence efforts as suggested by the 9/11 Commission to significantly improve information sharing and analysis. Several models to achieve this result exist, and despite the unique missions of the intelligence community can readily be adapted to guide this transformation.

We at the GAO stand ready to constructively engage with the intelligence community to share our significant government transformation and management knowledge and experience in order to help members of the community help themselves engage in the needed transformation efforts. We also stand ready to help the Congress enhance its oversight activities over the intelligence community, which, in our view, are an essential element of an effective transformation approach. In this regard, we have the people with the skills, experience, knowledge, and clearances to make a big difference for Congress and the country.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of your committee may have at this time.

[21] *V. Forging America's New Normalcy*, p. 2.

Contacts

For information on this testimony, please contact Randall Yim at (202) 512-6787 or yimr@gao.gov.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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