United States General Accounting Office

GAO

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

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

# COMBATING TERRORISM

# Evaluation of Selected Characteristics in National Strategies Related to Terrorism

Statement of Randall A. Yim, Managing Director
Homeland Security and Justice Issues

GAO-04-408T

February 3, 2004

# COMBATING TERRORISM

# Evaluation of Selected Characteristics in National Strategies Related to Terrorism

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-408T, testimony before the Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

## Why GAO Did This Study

Following the terrorist attacks of September 11, 2001, the Bush administration developed and published seven national strategies that relate, in part or in whole, to combating terrorism and homeland security. These were the:

- *National Security Strategy of the United States of America.*
- *National Strategy for Homeland Security.*
- *National Strategy for Combating Terrorism.*
- *National Strategy to Combat Weapons of Mass Destruction.*
- *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.*
- *National Strategy to Secure Cyberspace.*
- *2002 National Money Laundering Strategy.*

In view of heightened concerns about terrorism and homeland security, GAO was asked to identify and define the desirable characteristics of an effective national strategy and to evaluate whether the national strategies related to terrorism address those characteristics. The purpose of this testimony is to report on GAO's findings on this matter.

www.gao.gov/cgi-bin/getrpt?GAO-04-408T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Randall A. Yim at (202) 512-6787 or YimR@gao.gov.

## What GAO Found

National strategies are not required by either executive or legislative mandate to address a single, consistent set of characteristics. However, based on a review of numerous sources, GAO identified a set of desirable characteristics to aid responsible parties in further developing and implementing the strategies—and to enhance their usefulness in resource and policy decisions and to better assure accountability. The characteristics GAO identified are: (1) purpose, scope, and methodology; (2) problem definition and risk assessment; (3) goals, subordinate objectives, activities, and performance measures; (4) resources, investments, and risk management; (5) organizational roles, responsibilities, and coordination; and (6) integration and implementation.

GAO found considerable variation in the extent to which the seven strategies related to combating terrorism and homeland security address the desirable characteristics. A majority of the strategies at least partially address the six characteristics. However, none of the strategies addresses all of the elements of resources, investments, and risk management; or integration and implementation. Even where the characteristics are addressed, improvements could be made. For example, while the strategies identify goals, subordinate objectives, and specific activities, they generally do not discuss or identify priorities, milestones, or performance measures—elements that are desirable for evaluating progress and ensuring effective oversight. On the whole, the *National Strategy for Homeland Security* and the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* address the greatest number of desirable characteristics, while the *National Security Strategy* and the *National Strategy to Combat Weapons of Mass Destruction* address the fewest.

**The Pentagon in Flames Moments after International Terrorists Crash a Hijacked Aircraft into the Building on September 11, 2001**

Source: U.S. Marine Corps.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to be here today to participate in this hearing that examines the various national strategies published by the Bush Administration following the terrorist attacks of September 11, 2001. These strategies represent the administration's guidance to the federal state, local, private, and international sectors, for combating terrorism and securing the homeland and, equally important, for sustaining efforts into the future. Specifically, these seven strategies cover a broad range of related topics—from preparing against terrorist attacks to combating weapons of mass destruction, protecting our physical infrastructure, securing cyberspace, and blocking terrorist financing. The new strategies accompany the federal government's biggest reorganization in more than 50 years, resulting in the creation of a new Department of Homeland Security (DHS) to address the new threat environment.

Based upon heightened concerns about terrorism and homeland security, the Subcommittee asked us (1) to identify and define the characteristics of an effective national strategy and (2) to evaluate whether the strategies related to terrorism address those characteristics. This work expands upon our testimony to the Subcommittee in March 2003 and a related report in May 2003, as well as prior work for this Subcommittee and other committees over the past 7 years.[1]

After providing some background on the strategies related to terrorism, my statement will identify a set of desirable characteristics for any effective national strategy and compare and contrast the extent to which each of the strategies we address contains such characteristics. We believe these desirable characteristics would help shape the policies, programs, priorities, resource allocations, and standards that would enable federal agencies and other stakeholders to implement the strategies and achieve the identified results. We hope that the value of our review lies in assisting the evolution and implementation of these national strategies, so that homeland security efforts nationwide are clear, sustainable, and integrated into agency, governmental, and private sector missions; and, further, that

[1] See U.S. General Accounting Office, *Combating Terrorism*: *Observations on National Strategies Related to Terrorism*, GAO-03-519T (Washington, D.C.: Mar. 3, 2003) and *Combating Terrorism: Interagency Framework and Agency Programs to Address the Overseas Threat*, GAO-03-165 (Washington, D.C.: May 2003). In addition, a list of related GAO products is at the end of this statement.

these efforts are balanced with other important priorities, and transparent enough to ensure accountability.

We recognize the difficulty of the tasks presented to the strategy developers—and that national strategies are only starting points for federal agencies and other parties responsible for developing more detailed implementation plans. In some areas, so much needed to be done quickly that even general strategic statements added value. Some of the differences in detail in the national strategies may be attributed to their different breadths of scope and/or the maturity levels in their underlying program activities. We hope it is instructive to compare and contrast these strategies not only to each other, but also with other complex strategic planning efforts, so that the value of the strategies as guidance is enhanced and the timeframe for further refinements and implementation is expedited, given the critical nature of our homeland security efforts.

The new or updated national strategies released in the past 2 years that relate to combating terrorism and homeland security, in part or in whole, are:

- The *National Security Strategy of the United States of America*, September 2002.
- The *National Strategy for Homeland Security*, July 2002.
- The *National Strategy for Combating Terrorism*, February 2003.
- The *National Strategy to Combat Weapons of Mass Destruction*, December 2002.
- The *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*, February 2003.
- The *National Strategy to Secure Cyberspace*, February 2003.
- The *2002 National Money Laundering Strategy*, July 2002.

As agreed with your staff, we will report separately on the classified *National Military Strategic Plan for the War on Terrorism*.

## Summary

National strategies are not required by executive or legislative mandate to address a single, consistent set of characteristics, and they contain varying degrees of detail based on their different scopes. Furthermore, we found there was no commonly accepted set of characteristics used for an effective national strategy. Nonetheless, after consulting numerous sources, we identified a set of desirable characteristics that we believe would provide additional guidance to responsible parties for developing and implementing the strategies—and to enhance their usefulness as

guidance for resource and policy decision-makers and to better ensure accountability. Those characteristics are: (1) a statement of purpose, scope, and methodology; (2) problem definition and risk assessment; (3) goals, subordinate objectives, activities, and performance measures; (4) resources, investments, and risk management; (5) organizational roles, responsibilities, and coordination; and (6) integration and implementation. We identified these desirable characteristics by consulting statutory requirements pertaining to certain strategies we reviewed, as well as legislative and executive branch guidance for other national strategies. In addition, we studied the Government Performance and Results Act of 1993 (GPRA); general literature on strategic planning and performance; and guidance from the Office of Management and Budget (OMB) on the President's Management Agenda. We also gathered published recommendations made by national commissions chartered by Congress; past GAO work; and various research organizations that have commented on national strategies.

The seven national strategies related to homeland security and combating terrorism vary considerably in the extent to which they address the desirable characteristics that we identified. All seven strategies we reviewed partially address goals, subordinate objectives, activities, and performance measures. Four of the strategies address problem definition and risk assessment, while one strategy partially addresses that characteristic. And a majority of the strategies at least partially address the four other characteristics: purpose, scope, and methodology; resources, investments, and risk management; organizational roles, responsibilities, and coordination; and integration and implementation. However, none of the strategies addresses all of the elements of resources, investments, and risk management; or integration and implementation. Furthermore, even where the strategies address certain elements of the characteristics, there is room for improvement. For example, while the strategies identify goals, subordinate objectives, and specific activities, they generally do not discuss or identify priorities, milestones, or performance measures—elements that we consider to be desirable for evaluating progress, achieving results, and ensuring effective oversight. On the whole, the *National Strategy for Homeland Security* and the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* address the greatest number of the desirable characteristics, while the *National Security Strategy* and the *National Strategy to Combat Weapons of Mass Destruction* address the fewest. Table 1 shows the extent that the strategies address, partially address, or do not address our characteristics.

**Table 1: National Strategies and the Extent they Address GAO's Desirable Characteristics**

| National Strategy (short titles) | Purpose, scope, and methodology | Problem definition and risk assessment | Goals, subordinate objectives, activities, and performance measures | Resources, investments, and risk management | Organizational roles, responsibilities, and coordination | Integration and implementation |
|---|---|---|---|---|---|---|
| National Security | Does not address | Does not address | Partially addresses | Does not address | Does not address | Does not address |
| Homeland Security | Addresses | Addresses | Partially addresses | Partially addresses | Addresses | Partially addresses |
| Combating Terrorism | Partially addresses | Addresses | Partially addresses | Does not address | Partially addresses | Partially addresses |
| Weapons of Mass Destruction | Does not address | Does not address | Partially addresses | Does not address | Partially addresses | Partially addresses |
| Physical Infrastructure | Addresses | Addresses | Partially addresses | Partially addresses | Partially Addresses | Partially addresses |
| Secure Cyberspace | Partially addresses | Addresses | Partially addresses | Partially addresses | Partially Addresses | Partially addresses |
| Money Laundering | Partially addresses | Partially addresses | Partially addresses | Partially addresses | Partially addresses | Partially addresses |

Source: GAO analysis.

Note: Per our methodology, a strategy "addresses," a characteristic when it explicitly cites all elements of a characteristic, even if it lacks specificity and details and thus could be improved upon. A strategy "partially addresses" a characteristic when it explicitly cites some, but not all elements of a characteristic. Within our designation of "partially addresses" there is a wide variation between a strategy that addresses most of the elements of a characteristic and a strategy that addresses few of the elements of a characteristic. A strategy "does not address" a characteristic when it does not explicitly cite or discuss any elements of a characteristic, and/or any implicit references are either too vague or general. See appendix I for more details on our methodology.

# Background

## Seven National Strategies Related to Combating Terrorism Released Since September 11 Attacks

In the wake of the terrorist attacks on September 11, 2001, seven new national strategies were developed and published to help guide U.S. efforts to combat terrorism. Of these, five were newly published strategies that related to specific aspects of homeland security and combating terrorism, such as weapons of mass destruction, protecting physical infrastructure, and securing cyberspace. Two strategies, the *National Security Strategy of the United States of America* and *the 2002 National Money Laundering Strategy*, were updated from pre-September 11 versions to specifically include terrorism. "Terrorism" may be generally defined as

politically motivated violence to coerce a government or civilian population. "Combating terrorism" refers to the full range of policies, programs, and activities to counter terrorism, both at home and abroad. There is a further distinction within "combating terrorism," with "homeland security" referring to domestic efforts and "combating terrorism overseas" referring to international efforts.[2] Some of these national strategies were specific to combating terrorism, while others involved terrorism to lesser degrees. Table 2 describes the new national strategies related to combating terrorism.

**Table 2: National Strategies Related to Combating Terrorism**

| Strategy | Description of strategy |
|---|---|
| *National Security Strategy of the United States of America*<br>• Issued by the President, September 2002 | The *National Security* strategy provides a broad framework for strengthening U.S. security in the future. It identifies the national security goals of the United States, describes the foreign policy and military capabilities necessary to achieve those goals, evaluates the current status of these capabilities, and explains how national power will be structured to utilize these capabilities. It devotes a chapter to combating terrorism that focuses on the disruption and destruction of terrorist organizations, the winning of the "war of ideas," the strengthening of homeland security, and the fostering of cooperation with allies and international organizations to combat terrorism. |
| *National Strategy for Homeland Security*<br>• Issued by the President, July 2002 | The *Homeland Security* strategy addresses the threat of terrorism in the United States by organizing the domestic efforts of federal, state, local, and private organizations. It aligns and focuses homeland security functions into six critical mission areas, set forth as (1) intelligence and warning, (2) border and transportation security, (3) domestic counterterrorism, (4) protecting critical infrastructure and key assets, (5) defending against catastrophic threats, and (6) emergency preparedness and response. Additionally, it describes four foundations that cut across all the mission areas, across all levels of government, and across all sectors of society as being (1) law, (2) science and technology, (3) information sharing and systems, and (4) international cooperation. It also addresses the costs of homeland security and future priorities. |
| *National Strategy for Combating Terrorism*<br>• Issued by the President, February 2003 | The *Combating Terrorism* strategy elaborates on the terrorism aspects of the *National Security* strategy by expounding on the need to destroy terrorist organizations, win the "war of ideas," and strengthen security at home and abroad. Unlike the *Homeland Security* strategy that focuses on preventing terrorist attacks within the United States, the *Combating Terrorism* strategy focuses on identifying and defusing threats before they reach the borders of the United States. In that sense, although it has defensive elements, this strategy is an offensive strategy to complement the defensive *Homeland Security* strategy. |
| *National Strategy to Combat Weapons of Mass Destruction*<br>• Issued by the President, December 2002 | The *Weapons of Mass Destruction* strategy presents a national strategy to combat weapons of mass destruction (WMD) through three major efforts: (1) nonproliferation, (2) counterproliferation, and (3) consequence management in WMD incidents. The plan addresses the production and proliferation of WMD among nations, as well as the potential threat of terrorists using WMD agents. |

[2] For a more detailed discussion of the definition of terrorism, combating terrorism, and homeland security, see GAO-03-165.

| Strategy | Description of strategy |
|---|---|
| *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*<br>• Issued by the President, February 2003 | The *Physical Infrastructure* strategy provides a statement of national policy to remain committed to protecting critical infrastructures and key assets from terrorist attacks and is based on eight guiding principles, including establishing responsibility and accountability, encouraging and facilitating partnering among all levels of government and between government and industry, and encouraging market solutions wherever possible and government intervention when needed. The strategy also establishes three strategic objectives. The first is to identify and assure the protection of the most critical assets, systems, and functions, in terms of national level public health and safety, governance, and economic and national security and public confidence. The second is to ensure protection of infrastructures and assets facing specific, imminent threats. The third is to pursue collaborative measures and initiatives to ensure the protection of other potential targets that may become attractive over time. |
| *National Strategy to Secure Cyberspace*<br>• Issued by the President, February 2003 | The *Secure Cyberspace* strategy is intended to provide an initial framework for both organizing and prioritizing efforts to protect our nation's cyberspace. Also, it is to provide direction to federal departments and agencies that have roles in cyberspace security and to identify steps that state and local governments, private companies and organizations, and individual Americans can take to improve the nation's collective cybersecurity. The strategy is organized according to five national priorities, with major actions and initiatives identified for each. These priorities are: (1) a National Cyberspace Security Response System, (2) a National Cyberspace Security Threat and Vulnerability Reduction Program, (3) a National Cyberspace Security Awareness and Training Program, (4) Securing Governments' Cyberspace, and (5) National Security and International Cyberspace Security Cooperation. In describing the threats to, and vulnerabilities of, our nation's cyberspace, the strategy highlights the potential for damage to U.S. information systems from attacks by terrorist organizations. |
| *2002 National Money Laundering Strategy*<br>• Issued by the Secretary of the Treasury and the Attorney General, July 2002 | The *Money Laundering* strategy is intended to support planning for the efforts of law enforcement agencies, regulatory officials, the private sector, and overseas entities to combat the laundering of money generated from criminal activities. Although the 2002 strategy still addresses general criminal financial activity, that plan outlines a major governmentwide strategy to combat terrorist financing. The strategy discusses the need to adapt traditional methods of combating money laundering to unconventional tools used by terrorist organizations to finance their operations. |

Source: Published national strategies and GAO analysis.

## National Strategies Are Broad but Vary in Scope and Detail

These seven national strategies differ from other federal government planning documents, such as agency-specific strategic plans that GPRA requires.[3] These strategies are national in scope, cutting across levels of government and sectors and involving a large number of organizations and entities (i.e., the federal, state, local, and private sectors). In addition, national strategies frequently have international components, and they may be part of a structure of overlapping or supporting national strategies. Furthermore, the federal government does not control many of the sectors, organizations, entities, and resources involved in implementing the national strategies.

[3]P.L. 103-62 (Aug. 3, 1993).

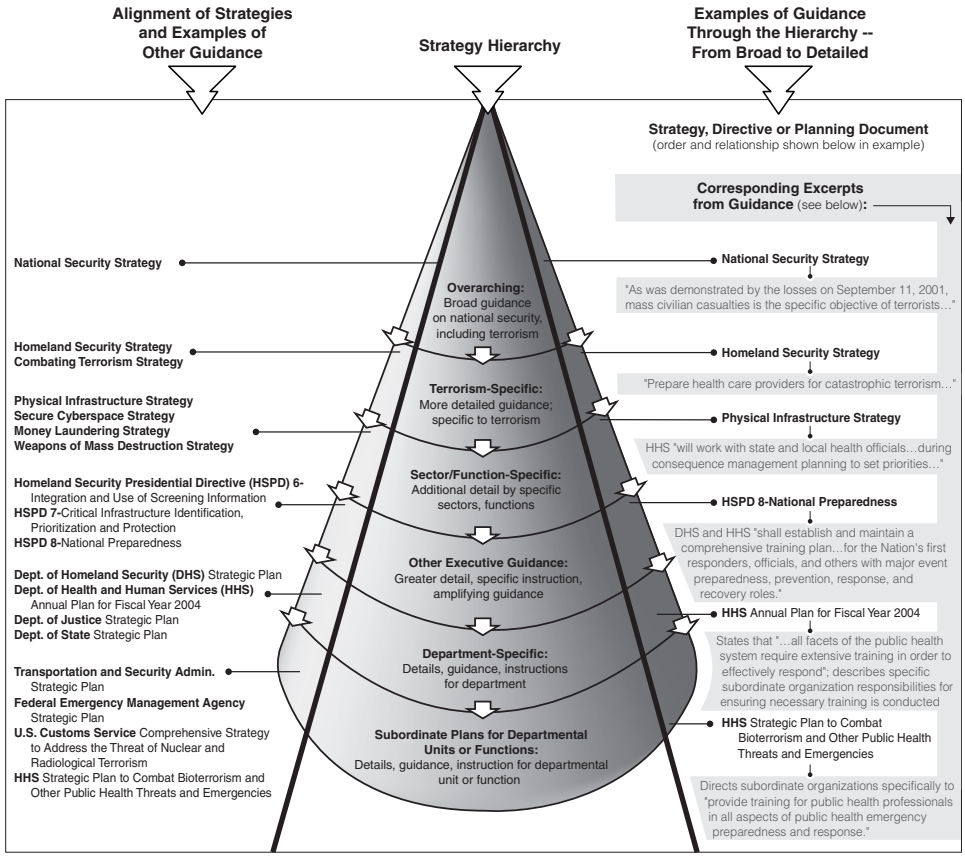
We found that the strategies we studied are organized in a rough hierarchy, with the *National Security* strategy providing an overarching strategy for national security as a whole, including terrorism. The *Homeland Security and Combating Terrorism* strategies provide, respectively, a more specific, defensive approach to combating terrorism at home and an offensive approach to combating terrorism overseas.[4] The other strategies provide further levels of detail on the specific functions related to weapons of mass destruction, cyber security, protection of physical infrastructure, and money laundering. While the national strategies we studied generally overlap in their coverage of terrorism, some contain elements unrelated to terrorism. For example, both the *Secure Cyberspace* and *Money Laundering* strategies include domestic criminal elements that are not necessarily associated with national security or terrorism.[5]

In addition, other executive branch guidance in the form of executive orders or presidential directives elaborates on the national strategies and provides further direction to the implementing parties. Most recently, for instance, the Homeland Security Presidential Directives 7 and 8, issued in December 2003, refine the national strategies with respect to critical infrastructure and national preparedness, respectively. In fact, those presidential directives identify specific priorities and milestones and assign certain responsibilities, which address some of our concerns on the lack of specificity and delineation of clear lines of responsibility in the national strategies. Further down the hierarchy, agency-specific strategic plans and performance plans; federal or agency-level enterprise architectures; and state, local, private and international sector plans provide even further details and guidance to implementing parties. In addition, these plans and reports may address goals and objectives beyond terrorism and homeland security. Figure 1 shows the hierarchy among the national strategies and other plans and guidance.

[4] We recognize that our characterization of these two strategies simplifies a complex relationship. Both strategies contain both defensive and offensive elements. For example, while we characterize the *Homeland Security* strategy as mainly defensive, it includes some offensive initiatives to target and attack terrorist financing, and to track foreign terrorists and bring them to justice. Similarly, while we characterize the *Combating Terrorism* strategy as mainly offensive, it includes some defensive objectives to implement the *Homeland Security* strategy and to protect U.S. citizens abroad.

[5] For example, the *Secure Cyberspace* strategy also covers nonterrorism-related computer hacking, and the *Money Laundering* strategy deals with all types of crimes associated with money laundering, such as drug trafficking.

**Figure 1. Hierarchy of National Strategies and Other Plans and Guidance for Combating Terrorism and Homeland Security**




Source: GAO.

## GAO Developed A Set of Desirable Characteristics for National Strategies

Because national strategies are not governed by a single, consistent set of requirements, we consulted a variety of public and private sector sources to identify a set of desirable characteristics. Those sources included legislative and executive branch mandates pertaining to the strategies we reviewed, as well as some nonterrorism-related strategies. We also studied GPRA; general literature on strategic planning and performance; and guidance from OMB on the President's Management Agenda. We also gathered published recommendations made by national commissions chartered by Congress; past GAO work; and various research organizations that have commented on national strategies. Based upon this methodology, we identified six characteristics to be desirable for a national strategy, which are described later in this testimony.

## No Single Set of Requirements in Place for Characteristics That National Strategies Should Contain

National strategies are not required, either by executive or legislative mandate, to address a single, consistent set of characteristics. Furthermore, we found that there is no commonly accepted set of characteristics used to develop an effective national strategy. Thus to identify desirable characteristics for all national strategies, including those related to terrorism, we consulted numerous sources. First, we identified statutory or executive requirements specific to some of the individual strategies for insight into whether those requirements could be generalized as desirable characteristics for all national strategies. Two of the seven strategies we reviewed—the *National Security* and *Money Laundering* strategies—are required by statutes that mandate specific content elements.[6]

The statute mandating the *Money Laundering* strategy generally calls for the strategy to contain provisions on setting goals, objectives, and priorities; coordinating prevention efforts; specifying detection and prosecution initiatives; and enhancing intergovernmental cooperation (at the federal, state, and local levels) and partnerships between the private sector and law enforcement agencies.[7] In addition, that statute calls for providing 3-year program projections and budget priorities; an assessment of how the budget is to be utilized and its sufficiency; the development of improved communication systems; and evaluations of the effectiveness of policies to combat money laundering and related financial crimes.

The statute mandating the *National Security* strategy calls for the document to provide a comprehensive description and discussion of U.S. worldwide interests, goals, and objectives vital to national security; detail the foreign policy, worldwide commitments, and national defense capabilities necessary to deter aggression and implement the strategy; identify the proposed short- and long-term uses of national power to protect our interests and achieve our goals and objectives; and assess the adequacy of our capabilities to carry out the national strategy.[8]

[6] Section 801(b) of the Homeland Security Act of 2002 requires DHS to develop a process for receiving meaningful input from states and localities to assist in the development of a national strategy "for combating terrorism and other homeland security activities," but does not establish specific content elements as do the laws pertaining to the *Money Laundering* and *National Security* strategies.

[7] 31 U.S.C. 5341.

[8] 50 U.S.C. 404a.

However, the requirements set forth in these two statutes, in addition to being different from one another, do not impose any requirements on the five other national strategies we reviewed.

## We Developed Characteristics Desirable for National Strategies

Given that there is no established set of requirements for all national strategies—or even the seven related specifically to homeland security and combating terrorism—we developed a set of desirable characteristics by reviewing several sources of information. First, we gathered statutory requirements pertaining to some of the strategies we were asked to assess—namely, the *Money Laundering* and the *National Security* strategies, as mentioned earlier—and legislative and executive branch guidance for other strategies, such as the *National Drug Control Strategy*. We also reviewed GPRA; general literature on strategic planning and performance; and guidance from OMB on the President's Management Agenda. Furthermore, we studied our past reports and testimonies for findings and recommendations pertaining to desirable elements of a national strategy. Similarly, we researched recommendations by national commissions chartered by Congress in recent years on combating terrorism and protecting the homeland—namely, the Bremer, Gilmore, and Hart-Rudman Commissions[9] —and various research organizations that have commented on national strategies.[10] Simultaneously, we consulted widely within GAO to incorporate the most up-to-date thinking on strategic planning; integration across and between government and its partners; implementation; and other related subjects. This included consulting our economists and methodologists to include cost-benefit analysis and other economic criteria. Furthermore, we consulted outside experts from the Bremer and Hart-Rudman Commissions. We used our judgment to develop desirable characteristics based upon their underlying support in legislative or executive guidance and the frequency with which they were cited in other sources. We then grouped similar items together

[9] Even before the terrorist attacks of September 11, 2001, Congress was concerned with the issue of homeland security and had chartered three national commissions, which examined terrorist threats and the government's response to terrorism, and made numerous recommendations. The full names of these commissions are the National Commission on Terrorism (also known as the Bremer Commission), the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (the Gilmore Commission), and the U.S. Commission on National Security/21st Century (the Hart-Rudman Commission).

[10] The research organizations whose work and commentary on homeland security, combating terrorism, and national strategies since 2000 that we primarily reviewed include the ANSER Institute on Homeland Security, RAND Corporation, and Brookings Institution.

in a logical sequence from conception to implementation. This was GAO's first effort to develop desirable characteristics for a national strategy, so they may evolve over time. Table 3 provides a summary of the six characteristics.

**Table 3: Summary of Desirable Characteristics for a National Strategy, from Conception to Implementation**

| Desirable characteristic | Description |
|---|---|
| Purpose, scope, and methodology | Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed. |
| Problem definition and risk assessment | Addresses the particular national problems and threats the strategy is directed towards. |
| Goals, subordinate objectives, activities, and performance measures | Addresses what the strategy is trying to achieve, steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results. |
| Resources, investments, and risk management | Addresses what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted based on balancing risk reductions with costs. |
| Organizational roles, responsibilities, and coordination | Addresses who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts. |
| Integration and implementation | Addresses how a national strategy relates to other strategies' goals, objectives, and activities, and to subordinate levels of government and their plans to implement the strategy. |

Source: GAO data.

We believe a national strategy should ideally contain all of these characteristics. Although the authors of national strategies might organize these characteristics in a variety of ways and/or use different terms, we present them in this order because they flow logically from conception to implementation. Specifically, the strategy's purpose leads to the definition of the problems and risks it intends to address, which in turn leads to specific actions for tackling those problems and risks, allocating and managing the appropriate resources, identifying different organizations' roles and responsibilities, and finally to integrating action among all relevant parties and implementing the strategy.

We describe the desirable characteristics in more detail in the following section, where we evaluate the extent to which the strategies address them. See appendix I for additional details on these characteristics and our scope and methodology in developing them.

## National Strategies Address Some, but Not All, of Desirable Characteristics GAO Identified

The seven national strategies related to homeland security and combating terrorism vary considerably in the extent to which they address the desirable characteristics that we identified. All seven strategies we reviewed partially address goals, subordinate objectives, activities, and performance measures. Four of the strategies address problem definition and risk assessment, while one strategy partially addresses that characteristic. And a majority of the strategies at least partially address the four other characteristics: purpose, scope, and methodology; resources, investments, and risk management; organizational roles, responsibilities, and coordination; and integration and implementation. However, none of the strategies addresses all of the elements of resources, investments, and risk management; or integration and implementation. Furthermore, even where the strategies address certain elements of the characteristics, there is room for improvement. For example, while the strategies identify goals, subordinate objectives, and specific activities, they generally do not discuss or identify priorities, milestones, or performance measures—elements that we consider to be desirable for evaluating progress, achieving results, and ensuring effective oversight. On the whole, the *National Strategy for Homeland Security* and the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* address the greatest number of the desirable characteristics, while the *National Security Strategy* and the *National Strategy to Combat Weapons of Mass Destruction* address the fewest.

We recognize that strategies themselves are not endpoints, but rather, starting points. In our view, the strengths of some strategies are useful in suggesting ways to enhance the value of other strategies, fill in gaps, speed implementation, guide resource allocations, and provide oversight opportunities. As with any strategic planning effort, implementation is the key. The ultimate measure of these strategies' value will be the extent they are useful as guidance for policy and decision-makers in allocating resources and balancing homeland security priorities with other important, nonhomeland security objectives. It will be important over time to obtain and incorporate feedback from the "user" community as to how the strategies can better provide guidance and how Congress and the administration can identify and remedy impediments to implementation, such as legal, international, jurisdictional, or resource constraints.

### Purpose, Scope, and Methodology

This characteristic addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed. For example, a strategy might discuss the specific impetus that led to its being written (or updated), such as statutory requirements, executive mandates, or other

events like terrorist attacks. Furthermore, a strategy would enhance clarity by including definitions of key, relevant terms (such as "combating terrorism," and "homeland security" in this context). In addition to describing what it is meant to do and the major functions, mission areas, or activities it covers, a national strategy would ideally address its methodology. For example, a strategy might discuss the principles or theories that guided its development, what organizations or offices drafted the document, whether it was the result of a working group, or which parties were consulted in its development.

Five of the national strategies we evaluated address at least some elements of this characteristic, with four at least partially discussing their overall purpose and scope, and three addressing, to varying degrees, their methodology. For example, the *Homeland Security* strategy explicitly identifies its fundamental objectives, coverage, and how it was developed. It describes itself as a framework to answer four basic questions—such as what is homeland security, and what goals it should pursue—and identifies six "critical mission areas," or homeland security functions, such as intelligence and warning, and border and transportation security. The *Physical Infrastructure*, *Secure Cyberspace*, and *Money Laundering* strategies also use explicit language to define their purposes and scope. For example, the *Physical Infrastructure* strategy identifies its scope as 13 critical sectors (such as agriculture, water, and public health) and five types of key assets (e.g., national monuments and dams). Concerning methodology, the *Homeland Security* strategy explicitly lays out the principles behind its creation and the numerous parties consulted in its development. Similarly, the *Physical Infrastructure* strategy explicitly discusses the guiding principles behind, and the consultations involved in, its creation. The *Combating Terrorism* and *Secure Cyberspace* strategies also describe their guiding principles—and the latter discusses, in even greater detail, the stakeholders involved in its development. And the *Money Laundering* strategy provides its background and highlights changes from the previous version to include terrorist financing.

However, three of the strategies discuss their purpose and scope only in vague terms, and four strategies do not address their methodology at all. For instance, regarding its purpose and scope, the *Weapons of Mass Destruction* strategy says only that, "The United States must pursue a comprehensive strategy to counter the WMD threat in all of its dimensions," without providing any further details. Similarly, while the *National Security* strategy emphasizes the importance of pursuing freedom, peace, and prosperity, it does not state its own purpose or scope. The *Combating Terrorism* strategy also uses vague language, such as "the

world must respond and fight this evil," but does not explicitly describe its purpose and scope. In addition, these three strategies, plus the *Money Laundering* strategy, do not discuss who was involved in their development. In our view, a complete description of the purpose, scope, and methodology in a national strategy could make the document more useful to the organizations responsible for implementing the strategy, as well as to oversight organizations, such as the Congress.

## Problem Definition and Risk Assessment

This characteristic addresses the particular national problems and threats the strategy is directed towards. Specifically, this means a detailed discussion or definition of the problems the strategy intends to address, their causes, and operating environment. In addition, this characteristic entails a risk assessment, including an analysis of the threats to, and vulnerabilities of, critical assets and operations.[11] If the details of these analyses are classified or preliminary, an unclassified version of the strategy could at least include a broad description of the analyses and stress the importance of risk assessment to implementing parties. A discussion of the quality of data available regarding this characteristic, such as known constraints or deficiencies, would also be useful.

Five of the strategies at least partially address this characteristic. Specifically, five define national problems and the environments in which they occur, while three discuss the importance of assessing risks, threats, and vulnerabilities. For example, the *Combating Terrorism* strategy contains an explicit section on "the nature of the terrorist threat today," which provides some historical background to terrorism, the structure of its leadership, and underlying conditions such as poverty, corruption, religious conflict, and ethnic strife. Similarly, the *Homeland Security*, *Physical Infrastructure*, *Secure Cyberspace*, and *Money Laundering* strategies define the problems in their sectors and describe the nature of the terrorist threat. Concerning risk assessment, three of them—the *Homeland Security*, *Physical Infrastructure*, and *Secure Cyberspace* strategies—stress the importance of national, comprehensive vulnerability

[11] This risk assessment is the first phase of a two-part risk management process. Risk assessment includes a threat assessment, a vulnerability assessment, and a criticality assessment. For a more in-depth discussion of these subjects, see U.S. General Accounting Office, *Homeland Security: Key Elements of a Risk Management Approach*, GAO-02-150T (Washington, D.C.: Oct.12, 2002). The second aspect of risk management is discussed below in the "Resources, Investments and Risk Management" characteristic. It consists of taking the information from the risk assessment and making management decisions about resource allocations to minimize risks and maximize returns on resources expended.

assessments of all critical infrastructures and key assets, setting the stage for risk management. The *Homeland Security* strategy contains an explicit "threat and vulnerability" section that provides many details, such as defining the different ways and means for terrorist attacks. This strategy also stresses the importance of comprehensive vulnerability assessments of all critical infrastructures and key assets, saying they "are important from a planning perspective in that they enable authorities to evaluate the potential effects of an attack on a given facility or sector, and then to invest accordingly in protecting such facilities and sectors."

However, two strategies do not address this characteristic. The *National Security* strategy says the war against terrorism is global and that "The enemy is not a single political regime or person or religion or ideology," but provides no further definition of the problems it seeks to address. Similarly, the *Weapons of Mass Destruction* strategy states that such weapons represent a great security challenge when in the possession of hostile states and terrorists, and that some terrorism-supporting states already possess such weapons, but provides no details defining the threat. Furthermore, while some of the strategies say that intelligence gathering must be strengthened, the strategies generally do not address limitations in collecting data. That is, few of the strategies discuss the difficulties of collecting intelligence on terrorist organizations, plans, and tactics. In our view, more specific information on both problem definition and risk assessment in many of the strategies would give the responsible parties better guidance to implement those strategies. For example, we recently recommended that future *Money Laundering* strategies link to periodic assessments of threats and risks, which would provide a basis for ensuring that clear priorities are established and focused on the areas of greatest need.[12]

Without necessarily prescribing in detail the "solution," better problem definition and risk assessment also provide greater latitude to responsible parties to develop innovative approaches that are tailored to the needs of specific regions or sectors—and are able to be implemented as a practical matter, given fiscal, human capital, and other limitations. For example, better problem definition or risk assessment can foster regional approaches or cooperative agreements, and stimulate the development of national systems or management standards to link the capabilities of the

[12] See U.S. General Accounting Office, *Combating Money Laundering: Opportunities Exist to Improve the National Strategy*, GAO-03-813 (Washington, D.C.: Sept. 2003).

responsible parties in a more effective manner. Such assessments help identify desired goals and "end-states" without "one-size-fits-all" solutions.

## Goals, Subordinate Objectives, Activities, and Performance Measures

This characteristic addresses what the national strategy strives to achieve and the steps needed to garner those results, as well as the priorities, milestones, and performance measures to gauge results. At the highest level, this could be a description of an ideal "end-state," followed by a logical hierarchy of major goals, subordinate objectives, and specific activities to achieve results. In addition, it would be helpful if the strategy discussed the importance of implementing parties' establishing priorities, milestones, and performance measures to help ensure accountability. Ideally, a national strategy would set clear desired results and priorities, specific milestones, and outcome-related performance measures while giving implementing parties flexibility to pursue and achieve those results within a reasonable timeframe. If significant limitations on performance measures exist, other parts of the strategy might address plans to obtain better data or measurements, such as national standards or indicators of preparedness. For example, national strategies related to terrorism might discuss the lack of national indicators or standards for emergency preparedness against attacks.

All seven national strategies partially address this characteristic by identifying their individual, high-level goals, subordinate objectives, and specific activities to achieve results.[13] For example, the *Homeland Security* strategy identifies three major goals—prevent terrorist attacks, reduce vulnerability, and minimize damage and recover from attacks—which are underpinned by six objectives (called critical mission areas), such as intelligence and warning, and border and transportation security. Those objectives in turn, have anywhere from 5 to 12 accompanying activities apiece. Figure 2 illustrates an example of an overall goal, subordinate objective, and specific activity in the *Homeland Security* strategy.

[13] The strategies differ in their terminology for goals, objectives, and activities. For example, some strategies refer to their top-level vision as "goals," while others describe that as "objectives." The same is true at the next level of support—some are called objectives, while others are "priorities" or "critical mission areas"—and at the most detailed level of activities (alternatively called "priorities" or "initiatives"). For the purpose of consistency in this testimony, we are using the terms "goals," "subordinate objectives," and "activities" (in order of broad to specific).

**Figure 2: The Homeland Security strategy contains an overall goal on recovering from terrorist attacks, a subordinate objective on emergency preparedness and response, and a specific initiative to prepare for chemical, biological, and nuclear decontamination**

Source: GAO.

Similarly, the *Combating Terrorism* strategy contains four overarching goals: defeat terrorists and their organizations; deny sponsorship, support, and sanctuary to terrorists; diminish the underlying conditions that terrorists seek to exploit; and defend U.S. citizens and interests at home and abroad. These goals are broken down into 15 objectives, such as

identifying terrorists and terrorist organizations, and are further supported by one to four activities each. Concerning milestones, the *Money Laundering* strategy provides a few deadlines for specific activities, such as the Departments of Treasury and Justice conducting a study by April 2003 on how the Internet could be used by terrorist groups to raise money. In addition, the *Homeland Security* strategy calls for DHS to develop and coordinate implementation of a comprehensive national plan to protect infrastructure against terrorist attacks, building on baseline protection plans due by the end of fiscal year 2002.[14] Regarding performance measures, the *Homeland Security* and *Money Laundering* strategies provide some general language on the subject. For example, the former says that, "Every department or agency will create benchmarks and other performance measures by which we can evaluate our progress and allocate future resources." And the latter says that methods for measuring performance should be consistent with the President's Management Agenda, and that the Department of the Treasury will develop a "traffic light" scorecard to track performance and assess how well the strategies' initiatives are being implemented.

However, the strategies do not address this characteristic in that they generally lack priorities, milestones, or performance measures. Regarding priorities, only the *Homeland Security* strategy identifies a priority order by stressing the importance of four specific activities in the fiscal year 2003 budget. Five strategies do not designate specific priorities; and the *Money Laundering* strategy, as highlighted in our recent report, identifies more priorities than can be achieved in a reasonable timeframe and does not rank them in order of importance.[15] Concerning performance measures, only two of them—the *Homeland Security* and *Money Laundering* strategies—explicitly stress the importance of measuring performance or identify specific measures. As we said in an earlier testimony, the *Homeland Security* strategy's initiatives often do not provide a baseline set of performance goals and measures upon which to

[14] The Homeland Security Act of 2002 requires DHS to develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States (P.L. 107-296, sec. 201(d)(5). Consistent with the Act, section (27) of the Homeland Security Presidential Directive 7 requires the Secretary of Homeland Security to complete a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection that outlines national goals, objectives, milestones, and key initiatives by December 2004.

[15] See GAO-03-813.

assess and improve preparedness.[16] Similarly, we recently recommended that future *Money Laundering* strategies require the principal agencies to develop outcome-related performance measures that are linked to goals and objectives.[17] Also, we previously reported that neither the *Physical Infrastructure* nor the *Secure Cyberspace* strategies indicate timeframes or milestones for their overall implementation or for accomplishing specific actions or initiatives; nor do they establish performance measures for which entities can be held responsible.[18] We believe a better identification of priorities, milestones, and performance measures would aid implementing parties in achieving results in specific timeframes—and would enable more effective oversight and accountability.

## Resources, Investments, and Risk Management

This characteristic addresses what the strategy will cost, the sources and types of resources and investments associated with the strategy, and where those resources and investments should be targeted. Ideally, a strategy would also identify criteria and appropriate mechanisms to allocate resources, such as grants, in-kind services, loans, and user fees, based on identified needs. Alternatively, the strategy might identify appropriate "tools of government," such as regulations, tax incentives, and standards, to mandate or stimulate nonfederal organizations to use their unique resources. Furthermore, a national strategy would ideally elaborate on the risk assessment mentioned earlier and give guidance to implementing parties to manage their resources and investments accordingly—and begin to address the difficult but critical issues about who pays, and how such efforts will be funded and sustained in the future.

Four of the strategies we evaluated partially address this characteristic by identifying numerous resource and investment needs to achieve their goals and objectives, and by discussing, to varying degrees, risk management. The *Homeland Security* strategy goes even farther, devoting a chapter to this topic in which it identifies a general principle to allocate homeland security investments based upon balancing risk reductions and costs. For example, the strategy states, "Decisions on homeland security activities

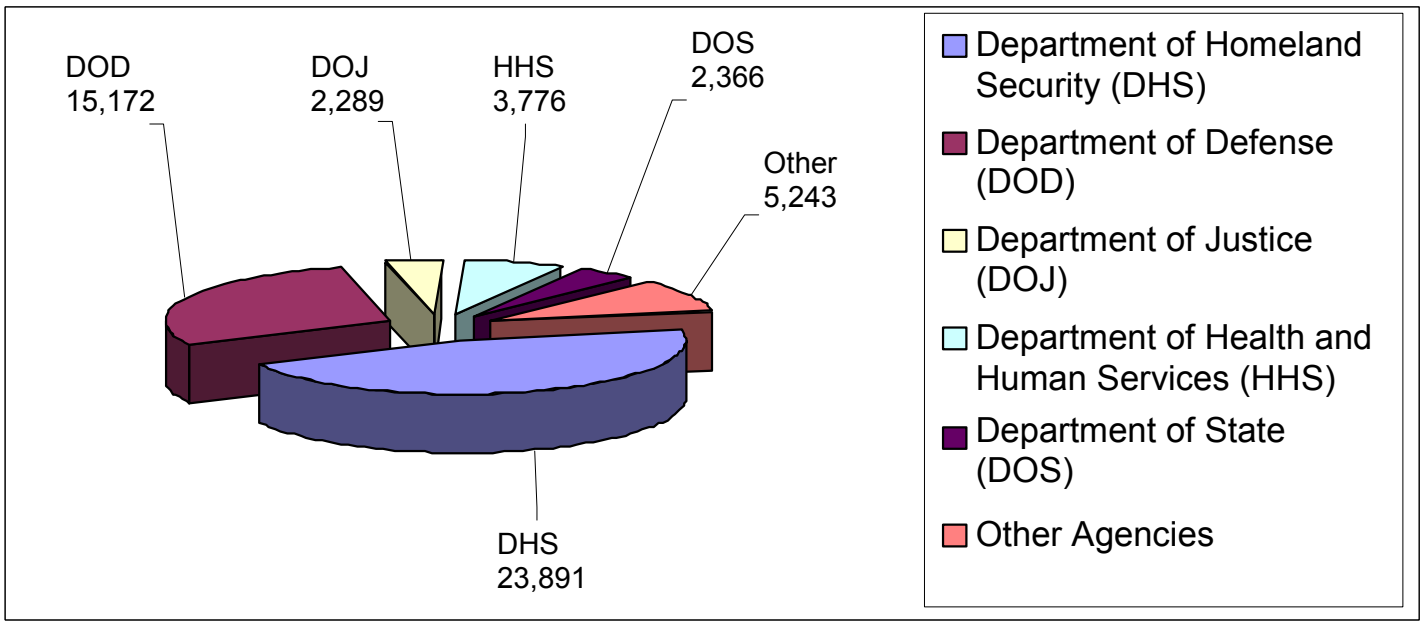
[16] See U.S. General Accounting Office, *Homeland Security: Effective Intergovernmental Coordination is Key to Success* GAO-02-1011T (Washington, D.C.: August 2002).

[17] See GAO-03-813.

[18] See U.S. General Accounting Office, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO-03-1165T (Washington, D.C.: September 2003).

and spending must achieve two overarching goals: to devote the right amount of scarce resources to homeland security and to spend these resources on the right activities." In addition, the *Homeland Security* strategy cites the concept that "the federal government will provide an incentive to minimize costs and reward innovation by permitting maximum flexibility in meeting those objectives." While the *Homeland Security* strategy cites these principles, it still provides relatively few details on the types and levels of resources associated with implementation. The *Physical Infrastructure* strategy also partially addresses this characteristic by identifying planning and resource allocation as one of its five objectives—and by stressing the importance of incentives for private organizations, and market solutions where appropriate. And the *Secure Cyberspace* strategy is one of only two strategies (the other being the *Homeland Security* strategy) to link some of its investment requests—such as completing the installation of the Cyber Warning and Information Network in key government operation centers—to the fiscal 2003 budget. The *Money Laundering* strategy also briefly discusses the importance of cost-benefit analysis of asset forfeiture strategies "so that future programs can allocate resources where they are most needed and productive." Figure 3 shows spending for combating terrorism by federal agency.

**Figure 3: Budget Authority for Combating Terrorism by Agency for Fiscal Year 2004 (total budget authority is $52,732 million)**




Source: OMB 2003 Report on Combating Terrorism.

Note: "Other Agencies" includes the Departments of Energy ($1,588 million), Agriculture ($368 million), Transportation ($283 million), Commerce ($153 million), Veterans Affairs ($145 million), Interior ($115 million), Treasury ($90 million), Labor ($67 million), Housing and Urban Development ($2 million), and 18 other independent agencies (totaling $2,432 million).

Regarding risk management, the *Homeland Security* strategy makes explicit reference to the subject, such as when it says, "The national effort to enhance homeland security will yield tremendous benefits and entail substantial financial and other costs." The *Physical Infrastructure* and *Secure Cyberspace* strategies also mention risk management, building on their aforementioned sections on risk assessment. In the former, for instance, increased sharing of risk-management expertise between the public and private sectors is an activity identified under the planning and resource allocation objective.

On the other hand, three of the strategies—the *National Security*, *Combating Terrorism*, and *Weapons of Mass Destruction* strategies—do not explicitly address either resource and investment needs or risk management. And of those that partially address this characteristic, only two—the *Homeland Security* and *Physical Infrastructure* strategies—provide explicit guidance or principles concerning resource allocation. Along those lines, none of the strategies provides cost estimates for

implementation in the aggregate, nor for specific goals, objectives, or activities. In addition, none of the strategies contains distinct chapters or sections, or detailed discussions of risk management. In our view, more guidance on resource, investment, and risk management would help implementing parties allocate resources and investments according to priorities and constraints, track costs and performance, and shift such investments and resources as appropriate. Such guidance would also assist Congress and the administration in developing more effective federal programs to stimulate desired investments, enhance preparedness, and leverage finite resources.

## Organizational Roles, Responsibilities, and Coordination

This characteristic addresses which organizations will implement the strategy, their roles and responsibilities, and mechanisms for coordinating their efforts. It helps answer the fundamental question about who is in charge, not only during times of crisis, but also during all phases of homeland security and combating terrorism efforts: prevention, vulnerability reduction, and response and recovery. This characteristic entails identifying the specific federal departments, agencies, or offices involved and, where appropriate, the different sectors, such as state, local, private, or international sectors. A strategy would ideally clarify implementing organizations' relationships in terms of leading, supporting, and partnering.[19] In addition, a strategy could describe the organizations that will provide the overall framework for accountability and oversight, such as the National Security Council, Homeland Security Council, OMB, Congress, or other organizations. Furthermore, a strategy might also identify specific processes for coordination and collaboration between sectors and organizations—and address how any conflicts would be resolved. For example, a strategy might also provide for some mechanism to ensure that the parties are prepared to fulfill their assigned responsibilities and use their available resources appropriately to enhance their capabilities and preparedness.

Six strategies at least partially address this characteristic. Specifically, two of them—the *Homeland Security* and *Physical Infrastructure* strategies—contain distinct chapters on "organizing," which discuss roles and responsibilities among the federal, state, local, private, and

[19] By "partnering," we refer to shared, or joint, responsibilities between implementing parties where there is otherwise no clear or established hierarchy of lead and support functions.

international sectors.[20] Furthermore, those two strategies, plus the *Secure Cyberspace* and *Money Laundering* strategies, frequently designate lead, and sometimes support, roles by objective, sector, or even specific activity.[21] Regarding accountability and oversight, the *Combating Terrorism* strategy identifies the creation of an international standard as one of its objectives, and the *Homeland Security* and *Physical Infrastructure* strategies highlight the importance of accountability. And concerning coordination between implementing parties, the *Homeland Security* and *Money Laundering* strategies designate some specific tools or processes (e.g., steering committee or task force), and the *Physical Infrastructure* strategy identifies the need to create collaborative mechanisms for government-industry planning; it also designates DHS as the primary liaison and facilitator for cooperation between all relevant parties.

On the other hand, the *National Security* strategy does not address this characteristic at all, and there is room for improvement in the other six strategies as well. For example, many of the references to U.S. roles and responsibilities in the *National Security* and *Combating Terrorism* strategies simply designate "the United States," rather than a specific federal agency, level of government, or sector. Thus those two strategies do not identify lead, support, and partner roles like the other strategies do. In addition, none of the strategies defines an overarching accountability or oversight framework, and five of the strategies do not identify specific tools or processes for coordination. For example, we recently recommended that future *Money Laundering* strategies address, among other things, strengthening the leadership structure and establishing a mechanism to resolve disputes among agencies and ensure accountability for implementation.[22] Also, we previously reported that neither the *Physical Infrastructure* nor the *Secure Cyberspace* strategies adequately define the roles, responsibilities, and relationships among the key critical infrastructure protection organizations, including state and local

[20] The *Homeland Security* strategy places many responsibilities on DHS, which had not been created yet when the strategy was published.

[21] The unclassified *Weapons of Mass Destruction* strategy outlines only a few specific responsibilities for the Homeland Security Council, National Security Council, and Department of State. However, its classified version contains more relevant details, which cannot be addressed in this unclassified statement.

[22] See GAO-03-813.

governments and the private sector.[23] The inclusion of these subjects in a national strategy would be useful to agencies and other stakeholders in fostering coordination and clarifying specific roles, particularly where there is overlap, and thus enhancing both implementation and accountability.

## Integration and Implementation

This characteristic addresses both how a national strategy relates to other strategies' goals, objectives, and activities—and to subordinate levels of government and their plans to implement the strategy. For example, a national strategy could discuss how its scope complements, expands upon, or overlaps with other national strategies, such as transportation infrastructure recapitalization or energy reliability. Similarly, related strategies could highlight their common or shared goals, subordinate objectives, and activities. In addition, a national strategy could address its relationship with relevant documents from implementing organizations, such as the strategic plans, annual performance plans, or annual performance reports required of federal agencies by GPRA. A strategy might also discuss, as appropriate, various strategies and plans produced by the state, local, private, or international sectors. It could also provide guidance such as the development of national standards to link together more effectively the roles, responsibilities, and capabilities of the implementing parties.

Five of the strategies address certain elements of this characteristic. Specifically, in terms of integration, the *Homeland Security* strategy states that it complements the *National Security* strategy in providing a framework for other security-related strategies and, in this vein, lays out goals, objectives, and mission areas that are shared with other strategies. The *Combating Terrorism*, *Weapons of Mass Destruction*, and *Secure Cyberspace* strategies also address integration by discussing the importance of other strategies and their complementary relationships. The *Homeland Security* and *Physical Infrastructure* strategies also provide some language on this subject, such as the latter's statement that DHS will collaborate with state and local governments as well as other federal agencies and the private sector to implement structures and processes for protecting assets and infrastructure. Regarding implementation, the *Homeland Security* strategy contains a distinct section on the subject, acknowledging that executive branch agencies need to issue detailed plans

[23] See GAO-03-1165T.

for the strategy's initiatives. And the *Money Laundering* strategy, for many of its activities, lists specific "action items" for agencies to implement. Two other strategies—the *Physical Infrastructure* and *Secure Cyberspace* strategies—make some general references to implementation. For example, the former says that "DHS and designated federal lead departments and agencies will prepare detailed implementation plans to support the activities outlined."

However, one of the strategies we reviewed—the *National Security* strategy—does not address this characteristic. It does not define its relationship to the other strategies; nor does it (along with the *Combating Terrorism*, *Weapons of Mass Destruction*, *Secure Cyberspace*, and *Money Laundering* strategies) address their relationship with other plans by federal, state, local, and other implementing parties. Furthermore, three strategies—the *National Security*, *Combating Terrorism*, and *Weapons of Mass Destruction* strategies—do not explicitly address implementation, and none of the strategies provides detailed guidance on the subject. We believe more information on this characteristic in a national strategy would build on the aforementioned organizational roles and responsibilities—and thus further clarify the relationships between various implementing parties, both vertically and horizontally. This, in turn, would foster effective implementation and accountability.

## Concluding Observations

The seven national strategies addressing homeland security and combating terrorism that we discuss in this testimony were developed to help the United States respond to an array of potential threats brought sharply into focus after the terrorist attacks of September 11, 2001. We recognize that these strategies were issued to meet a variety of homeland security needs and, furthermore, that they were not required, for the most part, to address the characteristics that we consider to be desirable. In addition, we do not expect all of the strategies to provide the same degree of detail because of their different scopes; for example, we consider it appropriate for the *National Security* strategy to contain fewer specifics than the *Physical Infrastructure* or *Money Laundering* strategies. Nonetheless, in our view, it would be useful for all of the strategies to address each of the characteristics, which logically flow from conception to implementation, in order to provide guidance to the federal agencies and other parties responsible for achieving results, evaluating progress, and ensuring accountability. Even where the strategies address our characteristics, we have identified potential areas for improvement. The numerous examples that I have cited today of the characteristics' inclusion in the national

strategies may serve as a model for future versions of these and other strategies.

The ultimate value of these strategies will be determined through time as the strategies are implemented by the federal, state, local, private, and international sectors—and as homeland security actions are embedded or integrated into ongoing governmental and private sector missions in sustainable and balanced ways. To achieve these goals, it will continue to be important to solicit the feedback and input from all responsible parties—legislative, federal, state, local, private, and international—and to incorporate this information to better achieve the parties' shared goals of improved homeland security and national preparedness. We will continue our work for the Subcommittee to evaluate these national strategies and their implementation. In the coming weeks, we look forward to reporting on (1) the extent that these strategies address recommendations by national commissions and GAO, (2) the extent to which implementing agencies are incorporating the national strategies into their own plans, and (3) the challenges faced in implementing these national strategies.

Mr. Chairman, this concludes my prepared statement. I will be pleased to respond to any questions that you or other members of the Subcommittee may have.

# GAO Contact and Staff Acknowledgments

## GAO Contact

Randall Yim at (202) 512-6787

## GAO Acknowledgments

Individuals making key contributions to this statement include Stephen L. Caldwell, Sharon Caudle, Josey Ballenger, Heather MacLeod, Jared Hermalin, Wayne A. Ekblad, Amy Bernstein, and Christine Davis.

# Appendix I: Scope and Methodology

This appendix describes how we developed the characteristics that we consider to be desirable for a national strategy and how we used them to evaluate the national strategies related to combating terrorism and homeland security.

## Developing Desirable Characteristics for a National Strategy

There are no legislative or executive mandates identifying a uniform set of required or desirable characteristics for all national strategies, including those related to combating terrorism and homeland security. While two of the seven strategies we reviewed—the *National Security* and *Money Laundering* strategies—are required by statutes to include specific content elements, the requirements set forth in these two statutes, in addition to being different from one another, do not levy any requirements on the five other national strategies we reviewed.

Given that there is no established set of requirements for all national strategies—or even the seven related specifically to combating terrorism and homeland security—we identified a set of desirable characteristics by reviewing several sources of information. First, we gathered statutory requirements pertaining to some of the strategies we were asked to assess—namely, the *Money Laundering* and *National Security* strategies, as mentioned earlier—as well as legislative and executive branch guidance for other strategies, such as the *National Drug Control Strategy*. We also consulted the Government Performance and Results Act (GPRA) of 1993; general literature on strategic planning and performance;[1] and guidance from the Office of Management and Budget (OMB) on the President's Management Agenda. In addition, we studied our past reports and testimonies for findings and recommendations pertaining to desirable elements of a national strategy. Similarly, we researched recommendations by national commissions chartered by Congress in recent years on combating terrorism and protecting the homeland—namely, the Bremer, Gilmore, and Hart-Rudman Commissions—and various research organizations that have commented on national strategies, such as the ANSER Institute on Homeland Security, RAND Corporation, and Brookings Institution.

[1] Examples of such literature include John M. Bryson's book *Strategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement* (Jossey-Bass, 1995) and Edward Filiberti's article, *National Strategic Guidance: Do We Need a Standard Format?* (Parameters, U.S. Army War College, Autumn 1995).

Simultaneously, we consulted widely within GAO to incorporate the most up-to-date thinking on strategic planning, integration across and between government and its partners, implementation, and other related subjects. This included consulting our economists and methodologists to include cost-benefit analysis and other economic factors. Furthermore, we consulted outside experts from the Bremer and Hart-Rudman Commissions.

We used our judgment to develop desirable characteristics based on their underlying support in legislative or executive guidance and the frequency with which they were cited in other sources. We then grouped similar items together in a logical sequence, from conception to implementation. This is our first effort to develop desirable characteristics for an effective national strategy, so they may evolve over time. The desirable characteristics are:

- Purpose, scope, and methodology.
- Problem definition and risk assessment.
- Goals, subordinate objectives, activities, and performance measures.
- Resources, investments, and risk management.
- Organizational roles, responsibilities, and coordination.
- Integration and implementation.

Later in this appendix, we provide a more detailed description of the six characteristics, plus examples of elements that a strategy might include to address them. We believe a national strategy should ideally contain all of these characteristics. Although the authors of national strategies might organize them in a variety of ways and/or use different terms, we present the characteristics in this order as a logical flow from conception to implementation. Specifically, the strategy's purpose leads to the definition of the problems and risks it intends to address, which in turn leads to specific actions for tackling those problems and risks, allocating and managing the appropriate resources, identifying different organizations' roles responsibilities and, finally, to integrating action among all relevant parties and implementing the strategy.

One challenge we encountered in identifying and applying these characteristics was determining the appropriate level of specificity a national strategy might contain. We found that there was no consensus on this issue among the sources and experts we consulted. Furthermore, the strategies we reviewed vary in their scope of coverage—some are broad

strategies, while others focus on implementation—and thus their level of detail varies.[2] We recognize that by their nature, national strategies are intended to provide broad direction and guidance—rather than be prescriptive, detailed mandates—to the relevant implementing parties. Thus it is unrealistic to expect all of the national strategies to provide details on each and every key characteristic we identified. Nonetheless, we believe the more detail a strategy provides, the easier it is for the responsible parties to implement it and achieve its goals. Table 4 provides the desirable characteristics and examples of their elements.

**Table 4: GAO Desirable Characteristics for a National Strategy**

| Desirable Characteristic | Brief description | Examples of elements |
|---|---|---|
| Purpose, scope, and methodology | Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed. | • Statement of broad or narrow purpose, as appropriate.<br>• How it compares and contrasts with other national strategies.<br>• What major functions, mission areas, or activities it covers.<br>• Principles or theories that guided its development.<br>• Impetus for strategy, e.g. statutory requirement or event.<br>• Process to produce strategy, e.g. interagency task force; state, local, or private input.<br>• Definition of key terms. |
| Problem definition and risk assessment | Addresses the particular national problems and threats the strategy is directed towards. | • Discussion or definition of problems, their causes, and operating environment.<br>• Risk assessment, including an analysis of threats and vulnerabilities.<br>• Quality of data available, e.g. constraints, deficiencies, and "unknowns." |
| Goals, subordinate objectives, activities, and performance measures | Addresses what the strategy is trying to achieve, steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results. | • Overall results desired, i.e. "end-state."<br>• Hierarchy of strategic goals and subordinate objectives.<br>• Specific activities to achieve results.<br>• Priorities, milestones, and outcome-related performance measures.<br>• Specific performance measures.<br>• Process for monitoring and reporting on progress.<br>• Limitations on progress indicators. |

[2] For example, the strategies range from the high-level, "grand" strategy (e.g., the *National Security* strategy) to the mid-level strategies specific to terrorism (e.g., the *Homeland Security* and *Combating Terrorism* strategies) and, finally, to the more detailed, sector- or function-specific strategies geared towards implementation (e.g., the *Secure Cyberspace*, and *Money Laundering* strategies).

| Desirable Characteristic | Brief description | Examples of elements |
|---|---|---|
| Resources, investments, and risk management | Addresses what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted by balancing risk reductions and costs. | • Resources and investments associated with the strategy.<br>• Types of resources required, such as budgetary, human capital, information technology, research and development, contracts.<br>• Sources of resources, e.g., federal, state, local, and private.<br>• Economic principles, such as balancing benefits and costs.<br>• Resource allocation mechanisms, such as grants, in-kind services, loans, or user fees.<br>• "Tools of government," e.g., mandates or incentives to spur action.<br>• Importance of fiscal discipline.<br>• Linkage to other resource documents, e.g. federal budget.<br>• Risk management principles. |
| Organizational roles, responsibilities, and coordination | Addresses who will be implementing the strategy, what their roles will be compared to others, and mechanisms for them to coordinate their efforts. | • Roles and responsibilities of specific federal agencies, departments, or offices.<br>• Roles and responsibilities of state, local, private, and international sectors.<br>• Lead, support, and partner roles and responsibilities.<br>• Accountability and oversight framework.<br>• Potential changes to current organizational structure.<br>• Specific processes for coordination and collaboration.<br>• How conflicts will be resolved. |
| Integration and implementation | Addresses how a national strategy relates to other strategies' goals, objectives and activities – and to subordinate levels of government and their plans to implement the strategy. | • Integration with other national strategies (horizontal).<br>• Integration with relevant documents from implementing organizations (vertical).<br>• Details on specific federal, state, local, or private strategies and plans.<br>• Implementation guidance.<br>• Details on subordinate strategies and plans for implementation, e.g., human capital, and enterprise architecture. |

Source: GAO.

The following sections provide more detail on the six characteristics and our support of each of them.

## Purpose, Scope, and Methodology

This characteristic addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed. For example, a strategy might discuss the specific impetus that led to its being written (or updated), such as statutory requirements, executive mandates, or other events like terrorist attacks. Furthermore, a strategy would enhance clarity by including definitions of key, relevant terms (such as "homeland security" and "combating terrorism," in this context). In addition to

describing what it is meant to do and the major functions, mission areas, or activities it covers, a national strategy would ideally address its methodology. For example, a strategy might discuss the principles or theories that guided its development, what organizations or offices drafted the document, whether it was the result of a working group, or which parties were consulted in its development.

We found support for this characteristic in legislation mandating two of the seven national strategies as well as by related legislation, executive orders, and GAO and policy research organization publications. For example, provisions relating to "purpose, scope, and methodology" appear in the statutes mandating the *National Security*[3] and *Money Laundering* strategies[4] (e.g., the statute requiring the *Money Laundering* strategy sets forth 12 areas that the strategy shall address.) Other legislative and executive branch guidance justifying the inclusion of this characteristic in our typology include: statutory requirements and related government publications describing the required purpose, scope, and methodology for the *National Drug Control Strategy*;[5] GPRA legislation calling for a comprehensive mission statement in agency strategic plans;[6] and an executive order determining the purpose and scope of a national council/strategy on information infrastructure.[7] In addition, at least two of our testimonies have directly addressed the relevant purpose and scope issues to be included within a homeland security strategy (e.g., the strategy is to be "national" in scope; its purpose is to include setting overall priorities and goals for homeland security). [8] But, we also pointed out in a 2002 testimony, that based upon interviews with officials at a dozen federal agencies, a broadly accepted definition of homeland security does not exist and that further clarification is needed.[9] The Gilmore

[3] 50 U.S.C. 404a.

[4] 31 U.S.C. 5341.

[5] See Section 1005 of the Anti-Drug Abuse Act of 1988, P.L. 100-690 (Nov. 18, 1988).

[6] See P.L. 103-62, sec. 3 (Aug. 3, 1993).

[7] Executive Order 12864 (Sept. 15, 1993).

[8] See U.S. General Accounting Office, *Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains*, GAO-02-610 (Washington, D.C.: June, 2002), p. 9; and *Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will be Pivotal to Success*, GAO-02-886T (Washington, D.C.: June 25, 2002), p. 4.

[9] See U.S. General Accounting Office, *Homeland Security: Progress Made; More Direction and Partnership Sought*, GAO-02-490T (Washington, D.C.: Mar. 12, 2002), p. 9.

Commission and ANSER Institute for Homeland Security have also addressed aspects of "purpose, scope, and methodology" issues that need to be addressed in a national strategy (e.g., the Gilmore Commission indicates that the strategy should be functionally comprehensive and address the full spectrum of the nation's efforts against terrorism).[10]

## Problem Definition and Risk Assessment

This characteristic addresses the particular national problems and threats the strategy is directed towards. Specifically, this means a detailed discussion or definition of the problems the strategy intends to address, their causes, and operating environment. In addition, this characteristic entails a risk assessment, including an analysis of the threats to, and vulnerabilities of, critical assets and operations.[11] If the details of these analyses are classified or preliminary, an unclassified version of the strategy could at least include a broad description of the analyses and stress the importance of risk assessment to implementing parties. A discussion of the quality of data available regarding this characteristic, such as known constraints or deficiencies, would also be useful.

Again, we found support for this characteristic in a variety of sources. While we have not identified any legislation that requires use of this characteristic in the national strategies on combating terrorism and homeland security that we reviewed, the importance of this characteristic is supported by the Homeland Security Act of 2002, as well as other legislation, presidential directives, and GAO and policy research organization publications. For example, the Homeland Security Act of 2002 directs the Department of Homeland Security (DHS) to conduct comprehensive assessments of vulnerabilities, including risk

[10] Second Annual Report to The President and The Congress Of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (aka Gilmore Commission), *II. Toward A National Strategy For Combating Terrorism* (Dec. 15, 2000), p. 4; Ruth David, *Homeland Security: Building A National Strategy*, The Bridge, 32, 1 (Spring, 2002), p. 2.

[11] This risk assessment is the first phase of a two-part risk management process. Risk assessment includes a threat assessment, a vulnerability assessment, and a "criticality" analysis. For a more in-depth discussion of these subjects, see *Homeland Security: Key Elements of a Risk Management Approach*, GAO-02-150T (Washington, D.C.: Oct.12, 2002). The second aspect of risk management is discussed in the "Resources, Investments and Risk Management" characteristics. It consists of taking the information from the risk assessment and making management decisions about resource allocations to minimize risks and maximize returns on resources expended.

assessments;[12] GPRA requires the identification of key factors external to an agency that can significantly impact that agency's attainment of its goals and objectives; [13] Homeland Security Presidential Directive (HSPD) 7, which addresses critical infrastructure protection, contains a background section that defines problem areas, and assesses the national risk potential if such problem areas are not effectively addressed. Likewise, an earlier critical infrastructure directive, Presidential Decision Directive (PDD) 63 defines the growing concern about the nation's vulnerability.[14] Additionally, we testified in 2002 that use of common definitions promotes more effective intergovernmental operations and more accurate monitoring of expenditures, thereby eliminating problematic concerns.[15] We also said that a national homeland security strategy should be based on a comprehensive national threat and risk assessment.[16] The Gilmore Commission, ANSER, and RAND have all suggested the need to conduct threat assessments to the homeland.[17]

## Goals, Subordinate Objectives, Activities, and Performance Measures

This characteristic addresses what the national strategy strives to achieve and the steps needed to garner those results, as well as the priorities, milestones, and performance measures to gauge results. At the highest level, this could be a description of an ideal "end-state," followed by a logical hierarchy of major goals, subordinate objectives, and specific activities to achieve results. In addition, it would be helpful if the strategy discussed the importance of implementing parties' efforts to establish priorities, milestones, and performance measures which help ensure

[12] P.L. 107-296, sec. 201(d)(2).

[13] P.L. 103-62, sec. 3.

[14] *See* Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization and Protection, Dec. 17, 2003, and Presidential Decision Direction/NSC-63, Critical Infrastructure Protection, May 22, 1998. HSPD-7 states that it supersedes PDD/NS C-63 to the extent of any inconsistency.

[15] See GAO-02-490T.

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

[17] First Annual Report to The President and The Congress Of the Advisory Panel To Assess Domestic Response Capabilities For Terrorism Involving Weapons Of Mass Destruction (aka Gilmore Commission), *I. Assessing the Threat* (December 15, 1999), p. 55; Ruth David, *Homeland Security: Building a National Strategy*, The Bridge, 32, 1 (Spring, 2002), p. 4; Bruce Hoffman, *Combating Terrorism: In Search of a National Strategy* RAND Corporation, CT-175, March 2001, pp. 3,6-7.

accountability. Ideally, a national strategy would set clear desired results and priorities, specific milestones, and outcome-related performance measures while giving implementing parties flexibility to pursue and achieve those results within a reasonable timeframe. If significant limitations on performance measures exist, other parts of the strategy might address plans to obtain better data or measurements, such as national standards or indicators of preparedness.[18] For example, national strategies related to terrorism might discuss the lack of national indicators or standards for emergency preparedness against attacks.

As in the case of the first characteristic, we found support for this characteristic in legislation mandating the *Money Laundering* and *National Security* strategies, as well as support derived from related legislation, presidential directive, the President's Management Agenda, and GAO and policy research organization publications. Both the *National Security* strategy and the *Money Laundering* strategy statutes emphasize the need for goals and objectives, as well as operational initiatives to promote those goals and objectives. There is also related legislative and executive supporting guidance for this characteristic in the following: the *National Drug Control Strategy* legislation, which requires a complete list of goals, objectives, and priorities;[19] the Homeland Security Act of 2002, which requires DHS to develop, in connection with a national terrorism countermeasures strategy, comprehensive, research-based definable goals and annual measurable objectives and specific targets to accomplish and evaluate such goals;[20] GPRA, which requires federal agencies to set goals and objectives in their strategic plans;[21] PDD 63, which includes a statement of presidential intent and national goals; [22] and the President's Management Agenda of FY2002,[23] which describes OMB's work regarding program objectives. Additionally, we testified that a national strategy

[18] For more information on the importance of national indicators for measuring problems, see U.S. General Accounting Office, *Forum on Key National Indicators: Assessing the Nation's Position and Progress* (GAO-03-672SP, May 2003).

[19] See Section 1005 of the Anti-Drug Abuse Act of 1988, P.L. 100-690 (Nov. 18, 1988).

[20] See P.L. 107-296, sec. 302(2).

[21] See P.L. 103-62, sec. 3.

[22] See Presidential Decision Directive 63, Critical Infrastructure Protection, May 22, 1998.

[23] Office of Management & Budget, *The President's Management Agenda*, *Fiscal Year 2002*, p. 29

should establish goals, objectives, and performance measures.[24] The Gilmore Commission, Brookings Institution and ANSER Institute for Homeland Security also commented on the need for setting priorities (goals), measurable outcomes and assessment of activities toward these ends.

## Resources, Investments, and Risk Management

This characteristic addresses what the strategy will cost, the sources and types of resources and investments needed, and where those resources and investments should be targeted. Ideally, a strategy would also identify appropriate mechanisms to allocate resources, such as grants, in-kind services, loans, and user fees, based on identified needs. Alternatively, a strategy might identify appropriate "tools of government," such as regulations, tax incentives, and standards, to mandate or stimulate nonfederal organizations to use their unique resources. Furthermore, a national strategy might elaborate on the risk assessment mentioned earlier and give guidance to implementing parties to manage their resources and investments accordingly—and begin to address the difficult but critical issues about who pays, and how such efforts will be funded and sustained in the future. Furthermore, a strategy might include a discussion of the type of resources required, such as budgetary, human capital, information, information technology (IT), research and development (R&D), procurement of equipment, or contract services. A national strategy might also discuss linkages to other resource documents, such as federal agency budgets or human capital, IT, R&D, and acquisition strategies. Finally, a national strategy might also discuss in greater detail how risk management will aid implementing parties in prioritizing and allocating resources, including how this approach will create society-wide benefits and balance these with society-wide costs. Related to this, a national strategy might discuss the economic principle of risk-adjusted return on resources.

In similar fashion, we found support for this characteristic in legislation mandating the *Money Laundering* and *National Security* strategies. Additionally, this characteristic receives related legislative and executive support, and is further supported by GAO and research policy organization publications. The *Money Laundering* strategy legislation requires a 3-year projection for program and budget priorities and a "complete assessment"

[24] See U.S. General Accounting Office, *Combating Terrorism: Intergovernmental Partnership in a National Strategy to Enhance State and Local Preparedness*, GAO-02-547T (Washington, D.C.: March 22, 2002), p. 3, and GAO-03-519T, p. 17.

of how the proposed budget is intended to satisfy strategy implementation.[25] The *National Security* strategy legislation requires an evaluation of whether the nation's "capabilities" (political, economic, and military) are adequate to support the implementation process.[26] Related legislative and executive branch supporting guidance for this characteristic derives from: the budget and resource balance provisions of the *National Drug Control Strategy*; HSPD-8 provisions targeting resource priorities against perceived risk of attack;[27] and the integration of performance monitoring and budgetary decision-making in the President's Management Agenda of Fiscal Year 2002.[28] GAO has also discussed the importance of this characteristic in recent testimonies, suggesting that the executive branch should link resources to threats, using a risk management approach and that carefully constructed investment strategies are needed to make appropriate use of limited fiscal and human resources.[29] The Hart-Rudman Commission and the Gilmore Commission have similarly discussed the need for a homeland security strategy to be appropriately resourced;[30] ANSER likewise has indicated the need for a

[25] 31 U.S.C. 5341(b)(6), (7).

[26] 50 U.S.C. 404a(b)(3), (4).

[27] Homeland Security Presidential Directive/HSPD-8, National Preparedness, sec. (6), Dec. 17, 2003.

[28] Office of Management & Budget, *The President's Management Agenda*, *Fiscal Year 2002*, p. 29.

[29] See U.S. General Accounting Office, *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), p. 3; and GAO-03-519T, pp. 7-8.

[30] The U.S. Commission on National Security/21st Century (aka The Hart-Rudman Commission), *Seeking A National Strategy: A Concert for Preserving Security and Promoting Freedom: Phase II Report* (Ap. 15, 2000), p. 16; Second Annual Report to The President and The Congress Of the Advisory Panel to Assess Domestic Response Capabilities For Terrorism Involving Weapons Of Mass Destruction (aka Gilmore Commission), *II. Toward A National Strategy For Combating Terrorism* (Dec. 15, 2000), pp. iv, 5; Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (aka Gilmore Commission), *IV. Implementing the National Strategy* (Dec.15, 2002), p. 37.

strategy to be supported by a comprehensive budget plan that aligns resources with national priorities.[31]

## Organizational Roles, Responsibilities, and Coordination

This characteristic addresses what organizations will implement the strategy, their roles and responsibilities, and mechanisms for coordinating their efforts. It helps to answer the fundamental question about who is in charge, not only during times of crisis, but also during all phases of homeland security efforts: prevention, vulnerability reduction, and response and recovery. This characteristic entails identifying the specific federal departments, agencies, or offices involved and, where appropriate, the different sectors, such as state, local, private, or international sectors. A strategy would ideally clarify implementing organizations' relationships in terms of leading, supporting, and partnering.[32] In addition, a strategy should describe the organizations that will provide the overall framework for accountability and oversight, such as the Homeland Security Council, OMB, Congress, or other organizations. Furthermore, a strategy might also identify specific processes for coordination and collaboration between sectors and organizations—and address how any conflicts would be resolved.

We found support for this characteristic in the *Money Laundering* strategy legislation, which provides that the strategy must address the coordination of regulatory and enforcement efforts; the enhancement of cooperation between federal, state, and local officials, as well as private sector entities; and the improvement of communications systems.[33] This characteristic also enjoys broad support from related legislation, executive orders, presidential directives, and recent GAO and policy research organization publications. For example, the Homeland Security Act of 2002 charges DHS with various functions, including coordination with nonfederal entities and promotion of public-private partnerships, among

[31] Ruth David, *Homeland Security: Building a National Strategy*, *The* Bridge, 32, 1 (Spring, 2002), p. 3; David McIntyre, *The National Strategy for Homeland Security: Finding the Path Among the Trees*, ANSER Institute for Homeland Security, (July 19, 2002), pp. 4-5.

[32] By "partnering," we refer to shared, or joint, responsibilities among implementing parties where there is otherwise no clear or established hierarchy of lead and support functions.

[33] 31 U.S.C. 5341(b)(2), (4), (5) and (11).

other things.[34] In addition, the statute mandating the *National Drug Control Strategy* calls for cooperative efforts between federal, state, and local governments and private sector initiatives.[35] Furthermore, HSPD-6, HSPD-7, PPD 63, and National Security Decision Directive (NSDD) 207 each seek to delineate the roles and responsibilities of various federal agencies and department heads; and Executive Order 13228 and HSPD-1 seek to coordinate implementation of the national strategy.[36] In addition, we emphasized that a national strategy should define the roles of federal, state, and local governments as well as the private sector, and that a national strategy needs to provide both direction and guidance to governments and the private sector so that missions and contributions can be more appropriately coordinated.[37] The Gilmore Commission, ANSER, and the Brookings Institution have also discussed the need for clearly assigning roles, responsibilities, accountability, liaison, and coordination among intergovernmental agencies, multilateral institutions, and international organizations.[38]

## Integration and Implementation

This characteristic addresses both how a national strategy relates to other strategies' goals, objectives, and activities (horizontal integration)—and to subordinate levels of government and other organizations and their plans to implement the strategy (vertical integration). For example, a national strategy could discuss how its scope complements, expands upon, or

[34] See P.L. 107-296, sec. 102(c), (f).

[35] Anti-Drug Abuse Act of 1988, P.L. 100-690, sec. 1005(b)(2).

[36] See generally Homeland Security Presidential Directive/HSPD-6, Integration and Use of Screening Information, Sept. 16, 2003; Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, Dec. 17, 2003; Presidential Decision Directive/NSC-63, Critical Infrastructure Protection, May 22, 1998; National Security Decision Directive/NSDD-207, The National Program for Combating Terrorism, Jan. 20, 1986; Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council, Oct. 8, 2001; and Homeland Security Presidential Directive/HSPD-1, Organization and Operation of the Homeland Security Council, Oct. 29, 2001.

[37] See GAO-03-519T, pp. 15-16; and GAO-02-621T, p. 3.

[38] First Annual Report to The President and The Congress of the Advisory Panel To Assess Domestic Response Capabilities For Terrorism Involving Weapons of Mass Destruction (aka Gilmore Commission), *I*: *Assessing the Threat* (December 15, 1999), pp. x-xi; Ruth David, *Homeland Security: Building a National Strategy*, The Bridge, 32,1 (Spring, 2002), p. 5; Michael E. O'Hanlon et al., *Protecting the American Homeland: One Year On*, Brookings Institution, 2003, p. xxv.

overlaps with other national strategies. Similarly, related strategies could highlight their common or shared goals, subordinate objectives, and activities. In addition, a national strategy could address its relationship with relevant documents from implementing organizations, such as the strategic plans, annual performance plans, or annual performance reports GPRA requires of federal agencies. A strategy might also discuss, as appropriate, various strategies and plans produced by the state, local, private or international sectors. A strategy could also provide guidance such as the development of national standards to link together more effectively the roles, responsibilities, and capabilities of the implementing parties.

We found support for this characteristic in the *Money Laundering* strategy legislation, which requires the strategy to address how to enhance intergovernmental cooperation and the flow of information between federal, state, and local governments; the coordination of regulatory and enforcement efforts; and the role of the private sector in a more integrated approach.[39] Related legislative and executive support derives from the *National Drug Control Strategy* legislation, presidential directive and executive order. The *National Drug Control Strategy* statutory requirements call for improving the timely flow of information to federal agencies by enhancing the compatibility of automated information and communication systems.[40] In addition, HSPD-7 addresses coordination and integration,[41] and Executive Order 13228 states that executive departments and agencies shall, to the extent permitted by law, make available to the Homeland Security Council all necessary information relating to terrorist threats and activities within the United States.[42] We indicated that the national strategy would benefit from addressing how intergovernmental and private sector initiatives can be operationally coordinated and integrated and, specifically, that an "overarching, integrated framework" can help deal with issues of potential duplication, overlap and conflict.[43] Similarly, the Gilmore Commission defined a "New Normalcy" of vertical

[39] 31 U.S.C. 5341(b)(4), (5), and (11).

[40] Anti-Drug Abuse Act of 1988, P.L. 100-690, sec. 1005(b)(6).

[41] *See* Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, Dec. 17, 2003.

[42] Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council, sec. 3(b)(ii), Oct. 8, 2001.

[43] See GAO-02-1122T, p. 12; and GAO-03-260, p. 38.

and horizontal information and intelligence sharing and ANSER has called for federal program integration where possible.[44]

## Applying the Desirable Characteristics to the National Strategies

After developing the characteristics, we reviewed the content of each national strategy to determine the extent to which it satisfied each of the six desirable characteristics. We did this by first summarizing the structure of each strategy in terms of its overall goals, subordinate objectives, and specific initiatives. Next, we carefully read through each strategy to apply our characteristics and recorded our results on individual matrixes so we could compare characteristics across the strategies. Finally, we summarized our results on a matrix "snapshot," using our judgment to rate each national strategy on each characteristic. Strategies could obtain one of three potential scores: "addresses," "partially addresses" or "does not address." Per our methodology, a strategy "addresses," a characteristic when it explicitly cites all elements of a characteristic, even if it lacks specificity and details and thus could be improved upon. A strategy "partially addresses" a characteristic when it explicitly cites some, but not all elements of a characteristic. Within our designation of "partially addresses" there is a wide variation between a strategy that addresses most of the elements of a characteristic and a strategy that addresses few of the elements of a characteristic. A strategy "does not address" a characteristic when it does not explicitly cite or discuss any elements of a characteristic, and/or any implicit references are either too vague or general.

To verify our work, the members of the project team independently reviewed the matrix summaries at every stage and made adjustments accordingly. Specifically, the project team verified that examples of where

[44] Fifth Annual Report to The President and The Congress of the Advisory Panel To Assess Domestic Response Capabilities For Terrorism Involving Weapons of Mass Destruction (aka Gilmore Commission), *V: Forging America's New Normalcy*, December, 15, 2003, pp. i, iv; David McIntyre, *the National Strategy for Homeland Security: Finding the Path Among the Trees*, The ANSER Institute for Homeland Security, 2002, p. 7.

strategies “address” or “partially address” characteristics were valid and, furthermore, that we properly characterized the strategies as not addressing the characteristics. In addition, we asked other internal teams who are familiar with the strategies from past reports and testimonies to verify our summary analysis.

# GAO Related Products

## Management (including Intergovernmental Coordination, Fiscal & Strategic Planning)

*Terrorist Financing: U.S. Agencies Should More Systematically Assess the Use of Alternative Financing Mechanisms*. GAO-04-163. Washington, D.C.: November 14, 2003.

*Combating Money Laundering: Opportunities Exist to Improve the National Strategy*. GAO-03-813. Washington, D.C.: September 26, 2003.

*Combating Terrorism: Interagency Framework and Agency Programs to Address Overseas Threat*. GAO-03-165. Washington, D.C.: May 23, 2003.

*Combating Terrorism: Observations on National Strategies Related to Terrorism*. GAO-03-519T. Washington, D.C.: March 3, 2003.

*Major Management Challenges and Program Risks: Department of Homeland Security*. GAO-03-102. Washington, D.C.: January 1, 2003.

*Homeland Security: Management Challenges Facing Federal Leadership*. GAO-03-260. Washington, D.C.: December 20, 2002.

*Homeland Security: Information Technology Funding and Associated Management Issues*. GAO-03-250. Washington, D.C.: December 13, 2002.

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

*Homeland Security: Effective Intergovernmental Coordination is Key to Success*. GAO-02-1013T. Washington, D.C.: August 23, 2002.

*Homeland Security: Critical Design and Implementation Issues*. GAO-02-957T. Washington, D.C.: July 17, 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.

*Homeland Security: Responsibility and Accountability for Achieving National Goals*. GAO-02-627T. Washington, D.C.: April 11, 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: A Framework for Addressing the Nation's Issues*. GAO-01-1158T. Washington, D.C.: September 21, 2001.

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

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

*Combating Terrorism: How Five Countries Are Organized to Combat Terrorism*. GAO/NSIAD-00-85. Washington, D.C.: April 7, 2000.

## Emergency Preparedness and Response

*Bioterrorism: A Threat to Agriculture and the Food Supply*. GAO-04-259T. Washington, D.C.: November 19, 2003.

*Homeland Security: Challenges in Achieving Interoperable Communications for First Responders*. GAO-04-231T. Washington, D.C.: November 6, 2003.

*September 11: Overview of Federal Disaster to the New York City Area*. GAO-04-72. Washington, D.C.: October 31, 2003.

*Homeland Security: Reforming Federal Grants to Better Meet Outstanding Needs*. GAO-03-1146T. Washington, D.C.: September 3, 2003.

*Hospital Preparedness: Most Urban Hospitals Have Emergency Plans but Lack Certain Capacities for Bioterrorism Response*. GAO-03-924. Washington, D.C.: August 6, 2003.

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

*Bioterrorism: Adequacy of Preparedness Varies Across State and local Jurisdictions*. GAO-03-373. Washington, D.C.: April 7, 2003.

*Homeland Security: Intergovernmental Coordination and Partnerships Will Be Critical to Success*. GAO-02-899T. Washington, D.C.: July 1, 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.

*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.

*Homeland Security: Progress Made; More Direction and Partnership Sought*. GAO-02-490T. Washington, D.C.: March 12, 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-02-162T. Washington, D.C.: October 17, 2001.

*Bioterrorism: Review of Public Health and Medical Preparedness Programs*. GAO-02-149T. Washington, D.C.: October 10, 2001.

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

*Combating Terrorism: Issues in Managing Counterterrorist Programs*. GAO/T-NSIAD-00-145. Washington, D.C.: April 6, 2000.

## Border and Transportation Security

*Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers*. GAO-04-325T. Washington, D.C.: December 16, 2003.

*Aviation Security: Efforts to Measure Effectiveness and Strengthen Security Programs*. GAO-04-285T. Washington, D.C.: November 20, 2003.

*Aviation Security: Efforts to Measure Effectiveness and Address Challenges*. GAO-04-232T. Washington, D.C.: November 5, 2003.

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

*Coast Guard: New Communication System to Search and Rescue Faces Challenges*. GAO-03-1111. Washington, D.C.: September 30, 2003.

*Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining*. GAO-03-1173. Washington, D.C.: September 24, 2003.

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

*Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain*. GAO-03-1155T. Washington, D.C.: September 9, 2003.

*Transportation Security: Federal Action Needed to Enhance Security Efforts*. GAO-03-1154T. Washington, D.C.: September 9, 2003.

*Aviation Security: Progress Since September 11th and the Challenges Ahead*. GAO-03-1150T. Washington, D.C.: September 9, 2003.

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

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

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

*Transportation Security: More Federal Coordination Needed to Help Address Security Challenges*. GAO-03-843. Washington, D.C.: June 30, 2003.

*Homeland Security: Challenges Facing the Department of Homeland Security in Balancing Its Trade Facilitation and Border Protection Missions*. GAO-03-902T. Washington, D.C.: June 16, 2003.

*Transportation Security: Post 9/11 Initiatives and Long-Term Challenges*. GAO-03-616T. Washington, D.C.: April 1, 2003.

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

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

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

## Information Analysis and Infrastructure Protection

*Critical Infrastructure Protection: Challenges in Securing Control Systems*. GAO-04-140T. Washington, D.C.: October 1, 2003.

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

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

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

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

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

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

*Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructure*. GAO-03-121. Washington, D.C.: January 30, 2003.

*Homeland Security: Information Sharing Activities Face Continued Management Challenges*. GAO-02-1122T. Washington, D.C.: October 1, 2002.

*National Preparedness: Technology and Information Sharing Challenges*. GAO-02-1048R. Washington, D.C.: August 30, 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.

*Homeland Security: Key Elements of a Risk Management Approach*. GAO-02-150T. Washington, D.C.: October 12, 2001.

## Science and Technology; Chemical, Biological, Radiological, and Nuclear Countermeasures

*Nuclear Security: Federal and State Action Needed to Improve Security of Sealed Radioactive Sources*. GAO-03-804. Washington, D.C.: August 6, 2003.

*Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to be Strengthened*. GAO-03-752. Washington, D.C.: September 4, 2003.

*Nuclear Nonproliferation: U.S. and International Assistance Efforts to Control Sealed Radioactive Sources Need Strengthening*. GAO-03-638. Washington, D.C.: May 16, 2003.

*Homeland Security: Title III of the Homeland Security Act of 2002*. GAO-02-927T. Washington, D.C.: July 9, 2002.

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. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

## GAO's Mission

The General Accounting 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 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 e-mail alerts" under the "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

PRINTED ON RECYCLED PAPER