United States General Accounting Office

GAO

Testimony

Before the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, U.S. Congress

Statement for the Record
September 23, 2002
For Release on
October 1, 2002

HOMELAND SECURITY

Information Sharing Activities Face Continued Management Challenges

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

GAO-02-1122T

Messrs. Chairmen and Members of the Committees:

Since the September 11, 2001, terrorist attacks, both the Administration and Congress have focused on the performance of the intelligence community and whether intelligence and other information is effectively shared – between federal agencies, with state and local law enforcement and other officials, and with private entities – to prevent or respond to terrorist attacks. Both the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have, in their joint inquiry, helped to illuminate many issues from which lessons can be drawn to improve how our intelligence community and other homeland security stakeholders share, analyze, integrate and disseminate important information, both at home and overseas.

Today, governments at all levels, as well as private sector entities, recognize that they have a greater role to play in protecting the nation from terrorist attacks. To achieve this collective goal, homeland security stakeholders must more effectively work together to strengthen the process by which critical information can be shared, analyzed, integrated and disseminated to help prevent or minimize terrorist activities. The work of these committees and of others in Congress and the Administration in crafting solutions to leverage agencies' abilities and willingness to share timely, useful information is critical to the fundamental transformation required in our homeland security community to ensure an affordable, sustainable and broad-based response to new and emerging threats to our country.

In your request that GAO provide a statement for the record, you asked us to focus on the information sharing activities of the intelligence, law enforcement, and other agencies involved in homeland security, as well as the role of state and local governments and the private sector. You also requested that we provide a description and status of the principal recommendations we have made related to combating terrorism.

We have developed an extensive body of work on combating terrorism over the years and more recently we have issued a number of reports on homeland security. Based on GAO's *Strategic Plan* issued in January 2000, which included a new emphasis on addressing key emerging threats to national security in a post-Cold War environment, GAO issued many reports prior to September 11th on combating terrorism and related matters. At the request of Congress, or on our own initiative, we currently have more than 80 engagements under way to examine a variety of

homeland security issues. Our ongoing work includes evaluations of information sharing activities in homeland security, including reviews of airport and transportation security, seaport security and law enforcement agencies. However, as the committees are aware, GAO's work in evaluating the activities of the intelligence community historically has been limited, due in part to limitations imposed by the intelligence agencies and the small number of requests made by Congress. My statement today reflects this limitation on evaluations of the intelligence community and focuses more broadly on information sharing among various homeland security stakeholders.

In my testimony today, I will discuss (1) some of the challenges to effective information sharing, including the fragmentation of information analysis responsibilities, and technology and collaboration challenges, and (2) GAO's views on addressing these challenges through transformational strategies, including strengthening the risk management framework; refining the national strategy, policy, and guidance structures to emphasize collaboration and integration among homeland security stakeholders to achieve common goals; and bolstering the fundamental management foundation integral to effective public sector performance and accountability. The statement also includes an appendix that lists GAO's recommendations on combating terrorism and the status of their implementation, as well as a list of related products.

Challenges to Effective Information Sharing

The success of a homeland security strategy relies on the ability of all levels of government and the private sector to communicate and cooperate effectively with one another. Activities that are hampered by organizational fragmentation, technological impediments, or ineffective collaboration blunt the nation's collective efforts to prevent or minimize terrorist acts.

Information Sharing Fragmentation

GAO and other observers of the federal government's organization, performance, and accountability for combating terrorism and homeland security functions have long recognized the prevalence of gaps, duplication, and overlaps driven in large part by the absence of a central policy focal point, fragmented missions, ineffective information sharing, human capital needs, institutional rivalries, and cultural challenges. In recent years, GAO has made numerous recommendations related to changes necessary for improving the government's response to combating terrorism.[1] Prior to the establishment of the Office of Homeland Security (OHS), GAO found that the federal government lacked overall homeland security leadership and management accountable to both the President and Congress. GAO has also stated that fragmentation exists in both coordination of domestic preparedness programs and in efforts to develop a national strategy.[2]

GAO believes that the consolidation of some homeland security functions makes sense and will, if properly organized and implemented, over time lead to more efficient, effective, and coordinated programs, better information sharing, and a more robust protection of our people, borders, and critical infrastructure.[3] At the same time, even the proposed Department of Homeland Security (DHS), will still be just one of many players with important roles and responsibilities for ensuring homeland security. In addition, the creation of DHS will not be a panacea. It will create certain new costs and risks, which must be addressed.

As it is with so many other homeland security areas, it is also the case for intelligence and information sharing that there are many stakeholders who must work together to achieve common goals. Effective analysis, integration, and dissemination of intelligence and other information critical to homeland security requires the involvement of the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), the National Security Council (NSC), the National Security Agency (NSA), the Department of Defense (DOD), and a myriad of other agencies, and will also include the

[1]U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, D.C.: September 2001).

[2]U.S. General Accounting Office, *Combating Terrorism: Comments on Counterterrorism Leadership and National Strategy*, GAO-01-556T (Washington, D.C.: March 27, 2001).

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

proposed DHS. State and local governments and the private sector also have critical roles to play – as do significant portions of the international community. Information is already being shared between and among numerous government and private sector organizations and more can be done to facilitate even greater sharing, analyzing, integrating, and disseminating of information.

We have observed fragmentation of information analysis and sharing functions potentially requiring better coordination in many homeland security areas. For example, in a recent report on critical infrastructure protection (CIP), we indicated that some 14 different agencies or components had responsibility for analysis and warning activities for cyber CIP.[4] Our recent testimony on aviation security indicated that the Immigration and Naturalization Service (INS), FBI and the Department of State all need the capacity to identify aliens in the United States who are in violation of their visa status, have broken U.S. laws, or are under investigation for criminal activity, including terrorism.[5] GAO has also noted that information sharing coordination difficulties can occur within single departments, such as those addressed in our July 2001 review of FBI intelligence investigations and coordination within the Department of Justice.[6] Procedures established by the Attorney General in 1995 required, in part, that the FBI notify the Criminal Division and the Office of Intelligence Policy and Review whenever a foreign counterintelligence investigation utilizing authorized surveillance and searches develops "…facts or circumstances…that reasonably indicate that a significant federal crime has been, is being, or may be committed…." However, according to Criminal Division officials, required notifications did not always occur and often, when they did, were not timely. The Attorney General and the FBI issued additional procedures to address the coordination concerns and ensure compliance, but these efforts have not been institutionalized.

[4]U.S. General Accounting Office, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, GAO-02-474 (Washington, D.C.: July 15, 2002).

[5]U.S. General Accounting Office, *Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenges*, GAO-02-971T (Washington, D.C.: July 25, 2002).

[6]U.S. General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters Is Limited*, GAO-01-780 (Washington, D.C.: July 2001).

Technological Impediments

This country has tremendous resources at its disposal, including leading edge technologies, a superior research and development base, extensive expertise, and significant human capital resources.[7] However, there are substantial challenges in leveraging these tools and using them effectively to ensure that timely, useful information is appropriately disseminated to prevent or minimize terrorist attacks. One challenge is determining and implementing the right format and standards for collecting data so that disparate agencies can aggregate and integrate data sets. For example, Extensible Markup Language (XML) standards are one option for exchanging information among disparate systems.[8] Further, guidelines and procedures need to be specified to establish effective data collection processes, and mechanisms need to be put in place to make sure that this happens – again, a difficult task, given the large number of government, private, and other organizations that will be involved in data collection. Mechanisms will be needed to disseminate data, making sure that it gets into the hands of the right people at the right time. It will be equally important to disaggregate information in order to build baselines (normative models) of activity for detecting anomalies that would indicate the nature and seriousness of particular vulnerabilities. Additionally, there is a lack of connectivity between databases and technologies important to the homeland security effort. Databases belonging to federal law enforcements agencies, for example, are frequently not connected, nor are the databases of the federal, state, and local governments. In fact, we have reported for years on federal information systems that are duplicative and not well integrated.[9]

[7]U.S. General Accounting Office, *National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy*, GAO-02-811T (Washington, D.C.: June 7, 2002).

[8]XML is the universal format for structured documents and data on the Web that makes it easy for a computer to generate data, read data, and ensure that the data structure is unambiguous. XML avoids common pitfalls in language design: It is extensible, platform-independent, and supports internationalization and localization. XML is a flexible, nonproprietary set of standards for annotating or "tagging" information so that it can be transmitted over a network and readily interpreted by disparate systems. For more information on its potential use for electronic government initiatives, see U.S. General Accounting Office, *Electronic Government: Challenges to Effective Adoption of the Extensible Markup Language*, GAO-02-327 (Washington, D.C.: April 2002).

[9]U.S. General Accounting Office, *Information Technology: Enterprise Architecture Use Across the Federal Government Can Be Improved*, GAO-02-6 (Washington, D.C.: February 2002).

Ineffective Collaboration

Ineffective collaboration among homeland security stakeholders remains one of the principal impediments to integrating and sharing information in order to prevent and minimize terrorist attacks. The committees' joint inquiry staff's initial report detailing numerous examples of strategic information known by the intelligence community prior to September 11th highlights the need to better ensure effective integration, collaboration, and dissemination of critical material.[10] The joint inquiry staff's report focuses on the national intelligence community, but its implications are clearly evident for all homeland security stakeholders – government at all levels, as well as the private sector, must work closely together to analyze, integrate, and appropriately disseminate all useful information to the relevant stakeholders in order to combat terrorism and make the nation more secure.

GAO recognizes that this goal is easier to articulate than achieve and that some long-standing obstacles to improving information sharing between and among stakeholders at all levels will require significant changes in organizational cultures, shifts in patterns of access to and limitations on information, and improved processes to facilitate communication and interaction.

GAO's ongoing work illuminates some of the issues. For instance, officials from the Department of Justice, FBI, and the Office of the Secretary of Defense indicated that the vast majority of information—about 90 percent—is already publicly available, and that only about 10 percent of the information is classified, sensitive, or otherwise restricted. The officials said that the expectation for all homeland security participants to obtain actionable information (actionable intelligence is information that is specific enough to tell who, what, where, and when an attack will take place) is unrealistic because, in most cases, the data do not exist or cannot be recognized as actionable. These officials also said that they do share actionable information with appropriate entities, but must also balance the release of the information against the possibility of disclosures that may reveal the sources and methods used to collect the information.

Non federal officials tend to echo these concerns. Since September 11th, GAO has met with representatives of various state and local organizations

[10]U.S. Congress, House and Senate Select Intelligence Committees, *Joint Inquiry Staff Statement, Part I,* (Washington, D.C.: September 18, 2002).

and conducted dozens of case studies of transit authorities, port authorities, and pipeline safety commissions and others entities, as well as testified before and heard testimonies from federal, state, and local officials at 11 congressional field hearings around the country. State and local officials continue to be frustrated by difficulties in the communication and sharing of threat information among all levels of government. Some of the problems they cited include: limited access to information because of security clearance issues, the absence of a systematic top-down and bottom-up information exchange, and uncertainties regarding the appropriate response to a heightened alert from the new homeland security advisory system. It is clear that sharing, analyzing, integrating, and disseminating information needs to occur both in and between all levels of government -- and throughout organizations both vertically and horizontally.

A number of steps have been taken to address these issues, but clearly more needs to be done. Following the terrorist attacks of September 11th, a review by the Department of Justice found that America's ability to detect and prevent terrorism has been undermined significantly by restrictions that limit the intelligence and law enforcement communities' access to, and sharing of, information. The USA Patriot Act, enacted shortly after the terrorist attacks, was designed to address this problem through enhanced information sharing and updating information-gathering tools. The Patriot Act gives federal law enforcement agencies greater freedom to share information and to coordinate their efforts in the war on terrorism. Methods to use this authority are now being established and implemented, but the effectiveness of these changes will need to be evaluated.

Moreover, the private sector has a critical role in reducing our vulnerability from terrorists. The national strategy for homeland security states: "Government at the federal, state, and local level must actively collaborate and partner with the private sector, which controls 85 percent of America's infrastructure."[11] The strategy further states that the government at all levels must enable the private sector's ability to carry out its protection responsibilities through effective partnerships and designates the proposed DHS as the primary contact for coordination at the federal level.

[11]The White House, *The National Strategy for Homeland Security* (Washington, DC, July 16, 2002).

Recently, the President's Critical Infrastructure Protection Board issued a strategy recognizing that all Americans have a role to play in cyber security, and identifies the market mechanisms for stimulating sustained actions to secure cyberspace.[12] The strategy recommends that the federal government identify and remove barriers to public-private information sharing and promote the timely two-way exchange of data to promote increased cyberspace security. Although industry groups already exchange security data, confidentiality concerns over the release of information may limit private sector participation. For example, the technology industry has said that any security information shared with the government should be exempt from disclosure under the Freedom of Information Act, which provides that any person has the right to request access to federal agency records or information.

GAO has also reported on how public-private information sharing practices can benefit CIP. In a report issued last October, GAO cited a number of important practices, including:

- establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;
- developing standards and agreements on how information will be used and protected;
- establishing effective and appropriately secure communications mechanisms; and
- taking steps to ensure that sensitive information is not inappropriately disseminated, which may require statutory change.[13]

Clearly, these practices are applicable to intelligence and information sharing in the broadest sense—and for stakeholders. Effectively implementing these practices will require using the full range of management and policy tools.

[12]The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace*, Draft (Washington, D.C.: September 2002).

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

Addressing the Challenges

GAO believes that the challenges facing the homeland security community require a commitment to focus on transformational strategies, including strengthening the risk management framework, refining the strategic and policy guidance structure to emphasize collaboration and integration among all relevant stakeholders, and bolstering the fundamental management foundation integral to effective public sector performance and accountability. Implementation of these strategies along with effective oversight will be necessary to institutionalize and integrate a long-term approach to sustainable and affordable homeland security.

Comprehensive Risk and Threat Assessment Needed

The events of September 11th have clearly shown the need for a comprehensive risk and threat assessment. Such an assessment, which needs to be integrated at all levels within the homeland security community, is necessary to better protect the nation's people, borders, and property. As your committees' work indicates, threats are many, and sources are numerous.

A comprehensive assessment can help the nation to better understand and manage the risks associated with terrorism. Moreover, a comprehensive risk and threat assessment is critical to setting priorities and allocating resources. There is no such thing as zero risk and, therefore, hard choices must be made given our limited resources over the coming years.

Previously, GAO observed that the federal government has not effectively planned and implemented risk assessment and management efforts. We noted in testimony before Congress last October that individual federal agencies have efforts under way, but the results to date have been inconclusive.[14] In the past, we have recommended that the FBI and the DOD enhance their efforts to complete threat and vulnerability assessments and to work with state and local governments in order to provide comprehensive approaches. Although some of this work was accomplished, delays resulting from the September 11th attacks have prevented their completion. Nevertheless, assessments can help in efforts to pinpoint risks and reallocate resources: For example, after September 11th the Coast Guard conducted initial risk assessments of the nation's ports. The Coast Guard identified high-risk infrastructure and facilities

[14]U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: October 31, 2001).

within specific areas of operation, which helped it to determine how to deploy resources to better ensure harbor security.

The Administration clearly recognizes the importance of such assessments. The national homeland security strategy points out that vulnerability assessments must be an integral part of the intelligence cycle for homeland security activities. They would allow planners to project the consequences of possible terrorist attacks against specific facilities or different sectors of the economy or government. The strategy also states the U.S. government does not now perform comprehensive vulnerability assessments of all the nation's critical infrastructure and key assets.

Integration of Strategic and Policy Framework Needed

GAO has long advocated the development and implementation of a national strategy to integrate and manage homeland security functions. The national strategy for homeland security released by the Administration last summer recognizes information sharing and systems as key factors cutting across all mission areas in linking and more effectively using the nation's information systems to better support homeland security. The issuance of this strategy is a very important step. Moreover, information systems and processes will need to be better integrated to support the goals established by the strategy.

In our current world, we can no longer think of information sharing, analysis, integration, and dissemination in terms of just the traditional intelligence community. Today, a broader network for information sharing includes the traditional intelligence community, U.S. allies, other federal agencies, state and local governments, and the private sector. To optimize such a network, it is important to have a strong, strategic planning framework and a supporting policy structure.

In addition, the national strategy identified one key homeland security mission area as intelligence and warning to detect and prevent terrorist actions. The intent is to provide timely and useful actionable information based on the review and analysis of homeland security information. The national strategy describes a number of initiatives to better develop opportunities for leveraging information sharing among homeland security stakeholders, including:

- Integrate information sharing across the federal government. This initiative addresses coordinating the sharing of essential homeland security information, including the design and implementation of an

interagency information architecture to support efforts to find, track, and respond to terrorist threats. This effort is among the Administration's budget priorities for fiscal year 2004.

- Integrate information sharing across state and local governments, private industry, and citizens. This initiative describes efforts to disseminate information from the federal government to state and local homeland security officials. One effort, to allow the exchange of information on federal and state government Web sites, has been completed.

- Adopt common "meta-data" standards for electronic information relevant to homeland security. This initiative is intended to integrate terrorist-related information from government databases and allow the use of "data mining" tools for homeland security. This effort is under way.

- Improve public safety emergency communications. This initiative is intended to develop comprehensive emergency communications systems that can disseminate information about vulnerabilities and protective measures and help manage incidents. State and local governments often report that there are deficiencies in their communications capabilities, including the lack of interoperable systems. Such systems are necessary between and among all levels of government. This effort is planned, but no timeline is indicated.

- Ensure reliable public health information. The last initiative is intended to address reliable communication between medical, veterinary, and public health organizations. It is under way.

While these initiatives provide a starting point for improved information sharing, their effective and timely implementation is not assured. A commitment to achieve these objectives must be emphasized. Implementation will require integration, coordination, and collaboration between organizations both within and outside the federal government. Further, the initiatives tend to rely on the creation of DHS for their complete implementation, a department that will require a considerable transition period to reach full potential. Improvements in efficiency and effectiveness are expected in the long term, but there will be additional costs and challenges, as the new department faces tremendous communications, human capital, information technology, and other integration, challenges.[15]

Moreover, it is also important to note that the national strategy for homeland security is one of several national strategies that address general and specific security and terrorism related issues. In addition to the homeland security strategy, the Administration recently released a national security strategy. The Administration has stated that the national security strategy could, in conjunction with the homeland security strategy, be viewed as an overarching framework. There are also requirements for several other strategies that cover specific aspects of national and homeland security. These include the National Strategy for Combating Terrorism, National Strategy to Combat Weapons of Mass Destruction, National Strategy to Secure Cyberspace, National Money Laundering Strategy, National Defense Strategy, and National Drug Control Strategy. These strategies reflect important elements supporting national and homeland security.

In is important that clear linkages be established among the various strategies to ensure common purpose within an overarching framework in order to clearly define specific roles, responsibilities, and resource priorities. An overarching, integrated framework can help to sort out issues of potential duplication, overlap, and conflict – not only for the federal government, but for all key stakeholders. While the individual plans will articulate roles and responsibilities, as well as set goals, objectives and priorities for their areas, effective integration is necessary to ensure that initiatives are undertaken that complement, not conflict with, each other.

[15]U.S. General Accounting Office, *Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will be Pivotal to Success*, GAO-02-886T (Washington, D.C.: June 25, 2002).

Further, integration would allow for the better utilization of resources. Given the many challenges we face, we do not have the resources do everything and must make some hard choices.

Finally, a comprehensive, integrated strategic framework requires a review of the policies and processes that currently guide sharing, analysis, integration, and dissemination of intelligence and other critical information to homeland security stakeholders. Indeed, the policy structure currently in place is principally the product of a Cold War environment, in which threats to the United States occurred mainly on foreign soil. New and emerging threats clearly demonstrate that terrorist acts can – and will – impact America at home. The changing nature of the threats present an opportunity for the homeland security community to revisit the legal and policy structure to ensure that it effectively creates an environment for the type of broad-based information sharing needed to protect America at home. It is not just the intelligence community, or the federal government, that have roles, as well as needs, in this evolving environment. Information can be collected by many sources and analyzed to identify potential threats. This information must be disseminated to all relevant parties – whether it is to a federal agency or another level of government. The volume and sources of threats, as your committees have reported, present new and serious challenges to our ability to analyze and integrate information into meaningful threat assessments. Not least, this will require attention to government's capacity to handle the increased volume of information.

Our policy structures need to adapt to these challenges. In fact, the government has recently implemented several measures that promote the sharing of information between all levels of government. For example, the USA Patriot Act provides for greater sharing of intelligence information among federal agencies. The FBI has also implemented several initiatives that would increase information sharing between all levels of government, including increasing the number of its Joint Terrorism Task Forces, to be located at each of its 56 field offices; and establishing the Terrorism Watch List to serve as its single, integrated list of individuals of investigative interest. The FBI plans to make the list accessible throughout the law enforcement and intelligence communities.

All of these are recent changes, of course, and will take time to fully implement. It will be important to assess how effective these and other changes are in promoting needed and appropriate information sharing. GAO stands ready to assist the Congress in these efforts.

Management Success Factors

As the recent proposals to create DHS indicate, the terrorist events of last fall have provided an impetus for the government to look at the larger picture of how it provides homeland security and how it can best accomplish associated missions – both now and over the long term. This imperative is particularly clear for the homeland security community, where information sharing and collaboration issues remain a challenge. In this environment, there exists a very real need and possibly a unique opportunity to rethink approaches and priorities to enable the homeland security community to better target its resources to address the most urgent needs. In some cases, the new emphasis on homeland security has prompted attention to long-standing problems that have suddenly become more pressing. In other cases, it will be equally important for organizations to focus on the fundamental building blocks necessary for effective public sector performance and accountability – foundations that readily apply to the homeland security community.

In recent months, we have testified about the long-term implementation challenges that the homeland security community faces – not only in ensuring an effective transition to a consolidated DHS, but in strengthening the relationships among and between all stakeholders to facilitate transformational change that can be sustained in years to come. There are many tools that organizations involved in homeland security might consider to drive necessary changes for better collaboration and integration of information sharing activities. One such tool is the Chief Operating Officer (COO) concept. Strategic positioning of COOs can provide a central point to elevate attention on management issues and transformational change, to integrate various key management functions and responsibilities, and to institutionalize accountability for management issues and leading change.

Despite some assertions to the contrary, there is no meaningful distinction between the intelligence community, other homeland security organizations, or even other public sector agencies when it comes to creating an environment where strong leadership and accountability for results drives a transformational culture. Over the years, GAO has made observations and recommendations about many success factors required for public sector effectiveness, based on effective management of people, technology, financial, and other issues, especially in its biannual Performance and Accountability Series on major government departments.[16] These factors include the following:

- Strategic Planning: Leading results-oriented organizations focus on the process of strategic planning that includes involvement of stakeholders, assessment of internal and external environments, and an alignment of activities, core processes and resources to support mission-related outcomes.

- Organizational Alignment: Operations should be aligned in a way that provides for effective sharing of information, consistent with the goals and objectives established in the national homeland security strategy.

- Communication: Effective communication strategies are key to any major transformation effort and help to instill an organizational culture that lends itself to effective sharing of information.

- Building Partnerships: A key challenge is the development and maintenance of homeland security partners at all levels of the government and the private sector, both in the United States and overseas.

- Performance Management: An effective performance management system fosters institutional, unit, and individual accountability.

- Human Capital Strategy: As with other parts of the government, homeland security agencies must ensure that their homeland security missions are not adversely impacted by the government's pending human capital crisis, and that they can recruit, retain, and reward a

[16] U.S. General Accounting Office, *Major Management Challenges and Program Risks: A Governmentwide Perspective*, GAO-01-241 (Washington, D.C.: January 2001).

talented and motivated workforce, which has required core competencies, to achieve their mission and objectives.

- Information Management and Technology: State-of-the art enabling technology is critical to enhance the ability to transform capabilities and capacities to share and act upon timely, quality information about terrorist threats.

- Knowledge Management: The homeland security community must foster policies and activities that make maximum use of the collective body of knowledge that will be brought together to determine and deter terrorist threats.

- Financial Management: All public sector entities have a stewardship obligation to prevent fraud, waste and abuse, to use tax dollars appropriately, and to ensure financial accountability to the President, Congress and the American people.

- Acquisition Management: The homeland security community, along with the proposed DHS, in the coming years will potentially have one of the most extensive acquisition requirements in government. High-level attention to strong systems and controls for acquisition and related business processes will be critical both to ensuring success and maintaining integrity and accountability.

- Risk Management: Homeland security agencies must be able to maintain and enhance current states of readiness while transitioning and transforming themselves into more effective and efficient collaborative cultures.

Creating and sustaining effective homeland security organizations will require strong commitment to these public sector foundations to foster our nation's safety.

Building Effective Systems

Of all the management success factors applicable to the homeland security community, one of the most important is the establishment of effective communications and information systems. Such systems will likely be critical to our efforts to build an integrated approach to information sharing. Meaningful understanding of inter- and intra-agency information sharing (intelligence or otherwise) necessitates the development of models depicting both how this occurs today and how this should occur tomorrow

to optimize mission performance. Such modeling is referred to as developing and implementing enterprise architectures, which in the simplest of terms can be described as blueprints (both business and technology) for transforming how an organization operates. Included in these architectures are information models defining, among other things, what information is needed and used by whom, where, when, and in what form. Without having such an architectural context within which to view the entity in question, a meaningful understanding of the strengths and weaknesses of information sharing is virtually impossible.

Currently, such an understanding within the homeland security arena does not exist. At OHS steps are being taken to develop enterprise architectures for each of the proposed department's four primary mission areas. According to the chief architect for this effort, working groups have been established for three of the four homeland security mission areas and they are in the process of developing business models (to include information exchange matrixes), that are based on the national strategy and that define how agencies currently perform these mission areas. For the fourth, which is information analysis and infrastructure protection (i.e., intelligence information sharing), the office is in the process of forming the working group. The goal of the groups is to follow OMB's enterprise architecture framework,[17] and deliver an initial set of architecture models describing how homeland security agencies operate by December 31, 2002.

Human Capital Emphasis

Human capital is another critical ingredient required for homeland security success. The government-wide increase in homeland security activities has created a demand for personnel with skills in areas such as information technology, foreign language proficiencies, and law enforcement – without whom, critical information has less chance of being shared, analyzed, integrated, and disseminated in a timely, effective manner. A GAO report issued in January 2002 stresses that foreign language translator shortages, combined in part with advances in technology, at some federal agencies have exacerbated translation backlogs in intelligence and other information. These shortfalls have adversely affected agency operations

[17]This framework provides for the following set of reference models: business, performance measures, data and information, application capabilities, and technology and standards.

and hindered U.S. military, law enforcement, intelligence, counter terrorism and diplomatic efforts.[18]

GAO believes it is reasonable for certain human capital and management flexibilities to be granted, provided that they are accompanied by adequate transparency and appropriate safeguards designed to prevent abuse and to provide for Congressional oversight. Such flexibilities might prove useful to other entities involved in critical information sharing activities. Moreover, the proposed department, similar to other federal agencies, would benefit from integrating a human capital strategy within its strategic planning framework. Naturally, this framework would apply to the intelligence community at large, as well as other homeland security stakeholders.

While recent events certainly underscore the need to address the federal government's human capital challenges, the underlying problem emanates from the longstanding lack of a consistent strategic approach to marshaling, managing, and maintaining the human capital needed to maximize government performance and assure government's accountability. Serious human capital shortfalls are eroding the capacity of many agencies, and threatening the ability of others to economically, efficiently, and effectively perform their missions. The federal government's human capital weaknesses did not emerge overnight and will not be quickly or easily addressed. Committed, sustained, and inspired leadership and persistent attention from all interested parties will be essential if lasting changes are to be made and the challenges we face successfully addressed.

GAO's model of strategic human capital management embodies an approach that is fact-based, focused on strategic results, and incorporates merit principles and other national goals. As such, the model reflects two principles central to the human capital idea:

- People are assets whose value can be enhanced through investment. As with any investment, the goal is to maximize value while managing risk.

- An organization's human capital approaches should be designed, implemented, and assessed by the standard of how well they help the

[18]U.S. General Accounting Office, *Foreign Languages: Human Capital Approach Needed to Correct Staffing and Proficiency Shortfalls*, GAO-02-375 (Washington, D.C.: January 2002).

organization pursue its mission and achieve desired results or outcomes.

The cornerstones to effective human capital planning include leadership; strategic human capital planning; acquiring, developing and retaining talent; and building results-oriented organizational cultures. The homeland security and intelligence communities must include these factors in their management approach in order to leverage high performance organizations in this critical time.

Institutional Oversight

Finally, it is important to note that the success of our nation's efforts to defend and protect our homeland against terrorism depends on effective oversight by the appropriate parts of our government. The oversight entities of the executive branch – including the Inspectors General, the OMB and OHS -- have a vital role to play in ensuring expected performance and accountability. Likewise, the committees of the Congress and the GAO, as the investigative arm of the legislative branch, have long term and broad institutional roles to play in supporting the nation's efforts to strengthen homeland security and prevent and mitigate terrorism. GAO recognizes the sensitive issues surrounding oversight of the intelligence and law enforcement communities, and we work collaboratively to find a balance between facilitating the needs of legitimate legislative oversight and preventing disclosure of national security and law enforcement sensitive information. Yet, as GAO has testified previously, our ability to be fully effective in our oversight role of homeland security, including the intelligence community, is at times limited. Historically, the FBI, CIA, NSA, and others have limited our access to information, and Congress's request for evaluations of the CIA have been minimal.[19] Given both the increasing importance of information sharing in preventing terrorism and the increased investment of resources to strengthen homeland security, it seems prudent that constructive oversight of critical intelligence and information sharing operations by the legislative branch be focused on the implementation of a long term transformation program and to foster information sharing in the homeland security community.

[19]U.S. General Accounting Office, *Central Intelligence Agency: Observations on GAO Access to Information on CIA Programs and Activities*, GAO-01-975T (Washington, D.C.: July 18, 2001).

In summary, I have discussed the challenges and approaches to improving information sharing among homeland security organizations, as well as the overall management issues that they face along with other public sector organizations. However, the single most important element of any successful transformation is the commitment of top leaders. Top leadership involvement and clear lines of accountability for making management improvements are critical to overcoming an organization's natural resistance to change, marshaling the resources needed to improve management, and building and maintaining organization-wide commitment to new ways of doing business. Organizational cultures will not be transformed, and new visions and ways of doing business will not take root without strong and sustained leadership. Strong and visionary leadership will be vital to creating a unified, focused homeland security community whose participants can act together to help protect our homeland.

This concludes my written testimony. I would be pleased to respond to any questions that you or members of the committees may have.

GAO Recommendations on Combating Terrorism and Homeland Security

This appendix provides a compendium of selected GAO recommendations for combating terrorism and homeland security and their status. GAO has conducted a body of work on combating terrorism since 1996 and, more recently, on homeland security. Many of our recommendations have been either completely or partially implemented, with particular success in the areas of (1) defining homeland security, (2) developing a national strategy for homeland security, (3) creating a central focal point for coordinating efforts across agencies, (4) tracking funds to combat terrorism, (5) improving command and control structures, (6) developing interagency guidance, (7) improving the interagency exercise program to maintain readiness, (8) tracking lessons learned to improve operations, (9) protecting critical infrastructure, (10) protecting military forces, (11) consolidating first responder training programs, (12) managing materials used for weapons of mass destruction, and (13) improving coordination of research and development. Overall, federal agencies have made realistic progress in many areas given the complexity of the environment confronting them. Many additional challenges remain, however, and some of GAO's previous recommendations remain either partially implemented or have not been implemented at all.

The information below details many of our key recommendations and the status of their implementation. The implementation of many of these recommendations may be affected by current proposals to transfer certain functions from a variety of federal agencies to the proposed Department of Homeland Security. Some of the recommendations have been modified slightly to fit into this format.

Combating Terrorism: Status of DOD Efforts to Protect Its Forces Overseas (GAO/NSIAD-97-207, July 21, 1997). Recommendations, p. 20.

GAO recommendations	Status of recommendations
We recommend that the Secretary of Defense direct the Chairman of the Joint Chiefs of Staff to develop common standards and procedures to include (1) standardized vulnerability assessments to ensure a consistent level of quality and to provide a capability to compare the results from different sites, (2) Department of Defense (DOD)-wide physical security standards that are measurable yet provide a means for deviations when required by local circumstances, and (3) procedures to maintain greater consistency among commands in their implementation of threat condition security measures.	Implemented. (1) The Joint Staff has sponsored hundreds of vulnerability assessments—known as Joint Staff Integrated Vulnerability Assessments—based on a defined set of criteria. (2) The Joint Staff has issued one volume of DOD-wide construction standards in December 1999, and plans to complete two additional volumes by December 2002. (3) DOD has provided more guidance and outreach programs to share lessons learned among commands.
To ensure that security responsibility for DOD personnel overseas is clear, we recommend that the Secretary of Defense take the necessary steps to ensure that the memorandum of understanding now under discussion with the Department of State is signed expeditiously. Further, the Secretary should provide the geographic combatant commanders with the guidance to successfully negotiate implementation agreements with chiefs of mission.	Implemented. The Departments of Defense and State have signed a memorandum of understanding, and scores of country-level memorandums of agreement have been signed between the geographic combatant commanders and their local U.S. ambassadors or chiefs of mission. These agreements clarify who is responsible for providing antiterrorism and force protection to DOD personnel not under the direct command of the geographic combatant commanders.

Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination (GAO/NSIAD-98-39, Dec. 1, 1997). Recommendations, p. 13.

GAO recommendations	Status of recommendations
We recommend that consistent with the responsibility for coordinating efforts to combat terrorism, the Assistant to the President for National Security Affairs of the National Security Council (NSC), in consultation with the Director, Office of Management and Budget (OMB), and the heads of other executive branch agencies, take steps to ensure that (1) governmentwide priorities to implement the national counterterrorism policy and strategy are established, (2) agencies' programs, projects, activities, and requirements for combating terrorism are analyzed in relation to established governmentwide priorities, and (3) resources are allocated based on the established priorities and assessments of the threat and risk of terrorist attack.	Partially implemented. (1) The Attorney General's Five-Year Counter-Terrorism and Technology Crime Plan, issued in December 1998, included priority actions for combating terrorism. According to NSC and OMB, the Five-Year Plan, in combination with Presidential Decision Directives (PDD) 39 and 62, represented governmentwide priorities that they used in developing budgets to combat terrorism. (2) According to NSC and OMB, they analyzed agencies' programs, projects, activities, and requirements using the Five-Year Plan and related presidential decision directives. (3) According to NSC and OMB, they allocated agency resources based upon the priorities established above. More recently, the Office of Homeland Security issued a National Strategy for Homeland Security, which also established priorities for combating terrorism domestically. However, there is no clear link between resources and threats because no national-level risk management approach has been completed to use for resource decisions.
To ensure that federal expenditures for terrorism-related activities are well-coordinated and focused on efficiently meeting the goals of U.S. policy under PDD 39, we recommend that the Director, OMB, use data on funds budgeted and spent by executive departments and agencies to evaluate and coordinate projects and recommend resource allocation annually on a crosscutting basis to ensure that governmentwide priorities for combating terrorism are met and programs are based on analytically sound threat and risk assessments and avoid unnecessary duplication.	Partially implemented. OMB now is tracking agency budgets and spending to combat terrorism. According to NSC and OMB, they have a process in place to analyze these budgets and allocate resources based upon established priorities. More recently, OMB also started tracking spending on homeland security—the domestic component of combating terrorism. However, there is no clear link between resources and threats. No national-level risk management approach has been completed to use for resource decisions.

Combating Terrorism: Opportunities to Improve Domestic Preparedness Program Focus and Efficiency (GAO/NSIAD-99-3, Nov. 12, 1998). Recommendations, p. 22.

GAO recommendations	Status of recommendations
We recommend that the Secretary of Defense—or the head of any subsequent lead agency—in consultation with the other five cooperating agencies in the Domestic Preparedness Program, refocus the program to more efficiently and economically deliver training to local communities.	Implemented. DOD transferred the Domestic Preparedness Program to the Department of Justice on October 1, 2000. The Department of Justice implemented this recommendation by emphasizing the program's train-the-trainer approach and concentrating resources on training metropolitan trainers in recipient jurisdictions. In June 2002, the President proposed that a new Department of Homeland Security take the lead for federal programs to assist state and local governments.
We recommend that the Secretary of Defense, or the head of any subsequent lead agency, use existing state and local emergency management response systems or arrangements to select locations and training structures to deliver courses and consider the geographical proximity of program cities.	Implemented. DOD transferred the Domestic Preparedness Program to the Department of Justice on October 1, 2000. The Department of Justice implemented this recommendation by modifying the programs in metropolitan areas and requiring cities to include their mutual aid partners in all training and exercise activities. In June 2002, the President proposed that a new Department of Homeland Security take the lead for federal programs to assist state and local governments.
We recommend that the National Coordinator for Security, Infrastructure Protection and Counterterrorism actively review and guide the growing number of weapons of mass destruction (WMD) consequence management training and equipment programs and response elements to ensure that agencies' separate efforts leverage existing state and local emergency management systems and are coordinated, unduplicated, and focused toward achieving a clearly defined end state.	Partially implemented. NSC established an interagency working group called the Interagency Working Group on Assistance to State and Local Authorities. One function of this working group was to review and guide the growing number of WMD consequence management training and equipment programs. In a September 2002 report, we reported that more needs to be done to ensure that federal efforts are coordinated, unduplicated, and focused toward achieving a clearly defined end state—a results-oriented outcome as intended for government programs by the Results Act. In June 2002, the President proposed that a new Department of Homeland Security take the lead for federal programs to assist state and local governments.

Combating Terrorism: Issues to Be Resolved to Improve Counterterrorism Operations (GAO/NSIAD-99-135, May 13, 1999).

GAO recommendations	Status of recommendations
We recommend that the Attorney General direct the Director, Federal Bureau of Investigation (FBI), to coordinate the Domestic Guidelines and concepts of operation plan (CONPLAN) with federal agencies with counterterrorism roles and finalize them. Further, the Domestic Guidelines and/or CONPLAN should seek to clarify federal, state, and local roles, missions, and responsibilities at the incident site.	Implemented. The Domestic Guidelines were issued in November 2000. The CONPLAN was coordinated with key federal agencies and was issued in January 2001.
We recommend that the Secretary of Defense review command and control structures, and make changes, as appropriate, to ensure there is unity of command to DOD units participating in domestic counterterrorist operations to include both crisis response and consequence management and cases in which they might be concurrent.	Implemented. In May 2001, the Secretary of Defense assigned responsibility for providing civilian oversight of all DOD activities to combat terrorism and domestic WMD (including both crisis and consequence management) to the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. Further, in October 2002, DOD will establish a new military command—the Northern Command—to manage command and control in domestic military operations to combat terrorism in support of other federal agencies.
We recommend that the Secretary of Defense require the services to produce after-action reports or similar evaluations for all counterterrorism field exercises that they participate in. When appropriate, these after-action reports or evaluations should include a discussion of interagency issues and be disseminated to relevant internal and external organizations.	Partially implemented. DOD has used its Joint Uniform Lessons Learned System to document observations and lessons learned during exercises, including interagency counterterrorist exercises. Many DOD units produce after-action reports and many of them address interagency issues. However, DOD officials acknowledged that service units or commands do not always produce after-action reports and/or disseminate them internally and externally as appropriate.

Combating Terrorism: Use of National Guard Response Teams Is Unclear (GAO/NSIAD-99-110, May 21, 1999). Recommendations, p. 20.

GAO recommendations	Status of recommendations
We recommend that the National Coordinator for Security, Infrastructure Protection and Counterterrorism, in consultation with the Attorney General, the Director, Federal Emergency Management Agency (FEMA), and the Secretary of Defense, reassess the need for the Rapid Assessment and Initial Detection teams in light of the numerous local, state, and federal organizations that can provide similar functions and submit the results of the reassessment to Congress. If the teams are needed, we recommend that the National Coordinator direct a test of the Rapid Assessment and Initial Deployment team concept in the initial 10 states to determine how the teams can best fit into coordinated state and federal response plans and whether the teams can effectively perform their functions. If the teams are not needed, we further recommend that they be inactivated.	Partially implemented. With authorization from Congress, DOD established additional National Guard teams and changed their names from Rapid Assessment and Initial Detection teams to WMD Civil Support Teams. However, subsequent to our report and a report by the DOD Inspector General, which found some similar problems, DOD agreed to review the National Guard teams and work with other agencies to clarify their roles in responding to terrorist incidents. In September 2001, DOD restricted the number of teams to 32.

Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attack (GAO/NSIAD-99-163, Sept. 7, 1999). Recommendations, p. 22.

GAO recommendations	Status of recommendations
We recommend that the Attorney General direct the FBI Director to prepare a formal, authoritative intelligence threat assessment that specifically assesses the chemical and biological agents that would more likely be used by a domestic-origin terrorist—nonstate actors working outside a state-run laboratory infrastructure.	Partially implemented. The FBI agreed with our recommendation. The FBI, working with the National Institute of Justice and the Technical Support Working Group, produced a draft threat assessment of the chemical and biological agents that would more likely be used by terrorists. FBI officials originally estimated it would be published in 2001. However, the terrorist attacks in the fall of 2001 delayed these efforts. The FBI and the Technical Support Working Group are now conducting an updated assessment of chemical and biological terrorist threats. According to the FBI, the assessment is being done by experts in WMD and terrorist training manuals and will include the latest information available. The assessment, once completed, will be disseminated to appropriate agencies.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
We recommend that the Attorney General direct the FBI Director to sponsor a national-level risk assessment that uses national intelligence estimates and inputs from the intelligence community and others to help form the basis for and prioritize programs developed to combat terrorism. Because threats are dynamic, the Director should determine when the completed national-level risk assessment should be updated.	Partially implemented. The Department of Justice and the FBI agreed to our recommendation. According to the FBI, it is currently working on a comprehensive national-level assessment of the terrorist threat to the U.S. homeland. The FBI said that this will include an evaluation of the chemical and biological weapons most likely to be used by terrorists and a comprehensive analysis of the risks that terrorist would use WMD. The FBI estimates the assessment will be completed in November 2002.

Combating Terrorism: Chemical and Biological Medical Supplies Are Poorly Managed (GAO/HEHS/AIMD-00-36, Oct. 29, 1999).
Recommendations, p. 10.

GAO recommendations	Status of recommendations
We recommend that the Department of Health and Human Services' (HHS) Office of Emergency Preparedness (OEP) and Centers for Disease Control and Prevention (CDC), the Department of Veterans Affairs (VA), and U.S. Marine Corps Chemical Biological Incident Response Force (CBIRF) establish sufficient systems of internal control over chemical and biological pharmaceutical and medical supplies by (1) conducting risk assessments, (2) arranging for periodic, independent inventories of stockpiles, (3) implementing a tracking system that retains complete documentation for all supplies ordered, received, and destroyed, and (4) rotating stock properly.	Partially implemented. Three of the recommendations have been implemented. However, only VA has implemented a tracking system to manage the OEP inventory. CDC is using an interim inventory tracking system. CBIRF has upgraded its database program to track medical supplies, and is working toward placing its medical supply operations under a prime vendor contract.

Combating Terrorism: Need to Eliminate Duplicate Federal Weapons of Mass Destruction Training (GAO/NSIAD-00-64, Mar. 21, 2000). Recommendations, p. 25.

GAO recommendations	Status of recommendations
We recommend that the Secretary of Defense and the Attorney General eliminate duplicate training to the same metropolitan areas. If the Department of Justice extends the Domestic Preparedness Program to more than the currently planned 120 cities, it should integrate the program with the Metropolitan Firefighters Program to capitalize on the strengths of each program and eliminate duplication and overlap.	Partially implemented. DOD transferred the Domestic Preparedness Program to the Department of Justice on October 1, 2000. The Department of Justice, while attempting to better integrate the assistance programs under its management, continued to run the Domestic Preparedness Program as a separate program. In June 2002, the President proposed that a new Department of Homeland Security take the lead for federal programs to assist state and local governments.

Combating Terrorism: Action Taken but Considerable Risks Remain for Forces Overseas (NSIAD-00-181, July 19, 2000). Recommendations, p. 26.

GAO recommendations	Status of recommendations
To improve the effectiveness and increase the impact of the vulnerability assessments and the vulnerability assessment reports, we recommend that the Secretary of Defense direct the Chairman of the Joint Chiefs of Staff to improve the vulnerability assessment reports provided to installations. Although the Joint Staff is planning to take some action to improve the value of these reports, we believe the vulnerability assessment reports should recommend specific actions to overcome identified vulnerabilities.	Not implemented. DOD believes that the changes in process at the time of our report addressed our recommendations. DOD is still in the process of implementing these actions.
To ensure that antiterrorism/force protection managers have the knowledge and skills needed to develop and implement effective antiterrorism/force protection programs, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to expeditiously implement the Joint Staff's draft antiterrorism/force protection manager training standard and formulate a timetable for the services to develop and implement a new course that meets the revised standards. Additionally, the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict should review the course content to ensure that the course has consistency of emphasis across the services.	Partially implemented. DOD revised its training standards for antiterrorism/force protection managers, but the Army has not implemented the new training standards.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
We recommend that the Joint Chiefs of Staff should develop an antiterrorism/force protection best practices or lessons learned program that would share recommendations for both physical and process-oriented improvements. The program would assist installations in addressing common problems—particularly those installations that do not receive Joint Staff Integrated Vulnerability Assessment reports or others who have found vulnerabilities through their own assessments.	Partially implemented. The Joint Chiefs of Staff have undertaken a number of lessons learned programs, but not all of the programs that would address this recommendation are operational.
To provide Congress with the most complete information on the risks that U.S. Forces overseas are facing from terrorism, we recommended that the Secretary of Defense direct the services to include in their next consolidated combating terrorism budget submission information on the number and types of antiterrorism/force protection projects that have not been addressed by the budget request and the estimated costs to complete these projects. Information on the backlog of projects should be presented by geographic command.	Not implemented. DOD did not concur with this recommendation. DOD believes that there is no need to provide the additional information to Congress.

Combating Terrorism: Federal Response Teams Provide Varied Capabilities; Opportunities Remain to Improve Coordination (GAO-01-14, Nov. 30, 2000). Recommendations, p. 27.

GAO recommendations	Status of recommendations
To guide resource investments for combating terrorism, we recommend that the Attorney General modify the Attorney General's Five-Year Interagency Counterterrorism and Technology Crime Plan to cite desired outcomes that could be used to develop budget requirements for agencies and their respective response teams. This process should be coordinated as an interagency effort.	Partially implemented. The Department of Justice asserted that the Five-Year Plan included desired outcomes. We disagreed with the department and believed what it cited as outcomes are outputs—agency activities rather than results the federal government is trying to achieve. The National Strategy for Homeland Security, issued in July 2002, supercedes the Attorney General's Five-Year Plan as the interagency plan for combating terrorism domestically. This strategy does not include measurable outcomes, but calls for their development.
We recommend that the Director, FEMA, take steps to require that the WMD Interagency Steering Group develop realistic scenarios involving chemical, biological, radiological, and nuclear agents and weapons with experts in the scientific and intelligence communities.	FEMA agreed with the recommendation. GAO is working with FEMA to determine the status of implementation. In June 2002, the President proposed that a new Department of Homeland Security take the lead for developing and conducting federal exercises to combat terrorism.
We recommend that the Director, FEMA, sponsor periodic national-level consequence management field exercises involving federal, state, and local governments. Such exercises should be conducted together with national-level crisis management field exercises.	FEMA agreed with the recommendation. GAO is working with FEMA to determine the status of implementation. In June 2002, the President proposed that a new Department of Homeland Security take the lead for developing and conducting federal exercises to combat terrorism.

Combating Terrorism: Accountability Over Medical Supplies Needs Further Improvement (GAO-01-463, Mar. 30, 2001). Recommendations, pp. 25 and 26.

GAO recommendations	Status of recommendations
We recommended that the Secretary of HHS require the Director of CDC to • execute written agreements as soon as possible with all CDC's partners covering the storage, management, stock rotation, and transporting of medical supplies designated for treatment of biological or chemical terrorism victims; • issue written guidance on security to private warehouses that store stockpiles; and • to the extent practical, install proper fencing prior to placing inventories at storage locations.	Partially implemented. CDC has implemented two of our recommendations and partially implemented one. Specifically, CDC has not finalized agreements with private transport companies to transport stockpiles in the event of a terrorist attack. It is currently using contracts between the federal government and the transport companies.
We recommend that the Secretary of HHS require the Director of OEP to • finalize, approve, and issue an inventory requirements list; • improve physical security at its central location to comply with Drug Enforcement Agency regulations, or move the supplies as soon as possible to a location that meets these requirements; • issue a written policy on the frequency of inventory counts and acceptable discrepancy rates; • finalize and implement approved national and local operating plans addressing VA's responsibilities for the procurement, storage, management, and deployment of OEP's stockpiles; • train VA personnel and conduct periodic quality reviews to ensure that national and local operating plans are followed; and • immediately contact Food and Drug Administration or the pharmaceutical and medical supply manufacturers of items stored at its central location to determine the impact of items exposed to extreme temperatures, replace those items deemed no longer usable, and either add environmental controls to the current location or move the supplies as soon as possible to a climate-controlled space.	Implemented. OEP has implemented all eight of our recommendations.
To ensure that medical supplies on hand reflect those identified as being needed to respond to a chemical or biological terrorism incident, we recommend that the Marine Corps Systems Command program funding and complete the fielding plan for the CBIRF specific authorized medical allowance list and that the Commandant of the Marine Corps require the Commanding Officer of CBIRF to adjust its stock levels to conform with the authorized medical allowance list and remove expired items from its stock and replace them with current pharmaceutical and medical supplies.	Implemented. CBIRF has implemented all of our recommendations.

Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities (GAO-01-323, Apr. 25, 2001). Recommendations, pp. 57, 68, and 85.

GAO recommendations	Status of recommendations
We recommend that the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies, • establish a capability for strategic analysis of computer-based threats, including developing a related methodology, acquiring staff expertise, and obtaining infrastructure data; • develop a comprehensive governmentwide data-collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources; and • clearly define the role of the National Infrastructure Protection Center (NIPC) in relation to other government and private-sector entities, including lines of authority among NIPC and NSC, Justice, the FBI, and other entities; NIPC's integration into the national warning system; and protocols that articulate how and under what circumstances NIPC would be placed in a support function to either DOD or the intelligence community.	Partially implemented. According to the NIPC director, NIPC has received sustained leadership commitment from key entities, such as the Central Intelligence Agency and the National Security Agency, and it continues to increase its staff primarily through reservists and contractors. The Director added that the NIPC (1) created an NIPC Senior Partners Group similar to a board of directors, which holds quarterly meetings with the senior leadership of each agency that details personnel to the NIPC in order to ensure that their interests are addressed with respect to future NIPC initiatives and program plans and to share with them the status of ongoing initiatives; (2) has developed close working relationships with other Critical Infrastructure Protection (CIP) entities involved in analysis and warning activities, such as the Federal Computer Incident Response Center (FedCIRC), DOD's Joint Task Force for Computer Network Operations, the Carnegie Mellon CERT® Coordination Center, and the intelligence and antivirus communities, and (3) had developed and implemented procedures to more quickly share relevant CIP information, while separately continuing any related law enforcement Investigation. In addition, the Director stated that two additional teams were created to bolster its analytical capabilities: (1) the critical infrastructure assessment team to focus efforts on learning about particular infrastructures and coordinating with respective infrastructure efforts and (2) the collection operations intelligence liaison team to coordinate with various entities within the intelligence community.
We recommend that the Attorney General task the FBI Director to require the NIPC Director to develop a comprehensive written plan for establishing analysis and warning capabilities that integrates existing planning elements and includes • milestones and performance measures; • approaches (or strategies) and the various resources needed to achieve the goals and objectives; • a description of the relationship between the long-term goals and objectives and the annual performance goals; and • a description of how program evaluations could be used to establish or revise strategic goals, along with a schedule for future program evaluations.	Partially implemented. The NIPC Director recently stated that NIPC has developed a plan with goals and objectives to improve its analysis and warning capabilities and that NIPC has made considerable progress in this area. The plan establishes and describes performance measures for both its Analysis and Warning Section and issues relating to staffing, training, investigations, outreach, and warning. In addition, the plan describes the resources needed to reach the specific goals and objectives for the Analysis and Warning Section. However, according According to NIPC officials, the NIPC continues to work on making its goals more measurable, better reflect performance, and better linked to future revisions to strategic goals.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
We recommend that the Attorney General direct the FBI Director to task the NIPC Director to • ensure that the Special Technologies and Applications Unit has access to the computer and communications resources necessary to analyze data associated with the increasing number of complex investigations; • monitor implementation of new performance measures to ensure that they result in field offices' fully reporting information on potential computer crimes to the NIPC; and • complete development of the emergency law enforcement plan, after comments are received from law enforcement sector members.	Partially implemented. According to NIPC officials, the Special Technologies and Applications Unit has continued to increase its computer resources. In addition, the director stated that the NIPC had developed and implemented procedures to more quickly share relevant CIP information, while separately continuing any related law enforcement investigation. However, because of the NIPC's reorganization in August 2002, when the Computer Investigation and Operations Section was moved from NIPC to the FBI's Cyber Crime Division, it is important that NIPC establish procedures to continue this information sharing. In addition, an emergency law enforcement services sector plan has been issued.
As the national strategy for critical infrastructure protection is reviewed and possible changes considered, we recommend that the Assistant to the President for National Security Affairs define NIPC's responsibilities for monitoring reconstitution.	The President's Critical Infrastructure Protection Board released a draft strategy on September 18, 2002, for comment. The draft states that a strategic goal is to provide for a national plan for continuity of operations, recovery, and reconstitution of services during a widespread outage of information technology in multiple sectors. However, NIPC's responsibilities regarding monitoring reconstitution are not discussed.
We recommend that the Assistant to the President for National Security Affairs (1) direct federal agencies and encourage the private sector to better define the types of information that are necessary and appropriate to exchange in order to combat computer-based attacks and procedures for performing such exchanges, (2) initiate development of a strategy for identifying assets of national significance that includes coordinating efforts already under way, such as those at DOD and Commerce, and (3) resolve discrepancies between PDD 63 requirements and guidance provided by the federal Chief Information Officers Council regarding computer incident reporting by federal agencies.	Partially implemented. NIPC officials told us that a new ISAC development and support unit had been created, whose mission is to enhance private-sector cooperation and trust, resulting in a two-way sharing of information. Officials informed us that NIPC has signed information sharing agreements with most of the ISACs formed, including those representing telecommunications, information technology, water supply, food, emergency fire services, banking and finance, and chemical sectors. NIPC officials added that most of these agreements contained industry-specific cyber and physical incident reporting thresholds. NIPC has created the Interagency Coordination Cell to foster cooperation across government agencies in investigative matters and on matters of common interest.
We recommend that the Attorney General direct the FBI Director to direct the NIPC Director to (1) formalize relationships between NIPC and other federal entities, including DOD and the Secret Service, and private-sector Informantion Sharing Analysis Centers (ISACs) so that a clear understanding of what is expected from the respective organizations exists, (2) develop a plan to foster the two-way exchange of information between the NIPC and the ISACs, and (3) ensure that the Key Asset Initiative is integrated with other similar federal activities.	Partially implemented. According to NIPC's Director, the relationship between NIPC and other government entities has significantly improved since our review, and the quarterly meetings with senior government leaders have been instrumental in improving information sharing. In addition, in testimony, officials from the FedCIRC and the U.S. Secret Service have discussed the collaborative and cooperative relationships that now exist between their agencies and NIPC. However, further work is needed to identify assets of national significance and coordinate with other similar federal activities.

FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters Is Limited (GAO-01-780, July 16, 2001). Recommendations, p. 32.

GAO recommendations	Status of recommendations
To facilitate better coordination of FBI foreign counterintelligence investigations meeting the Attorney General's coordination criteria, we recommend that the Attorney General establish a policy and guidance clarifying his expectations regarding the FBI's notification of the Criminal Division and types of advice that the division should be allowed to provide the FBI in foreign counterintelligence investigations in which the Foreign Intelligence Surveillance Act (FISA) tools are being used or their use is anticipated.	Partially implemented. In an August 6, 2001, memorandum, the Deputy Attorney General outlined the responsibilities of the FBI, Criminal Division, and the Office of Intelligence Policy and Review (OIPR) regarding intelligence sharing in FISA cases and issued clarifications to the Attorney General's 1995 coordination procedures. Specifically, these clarifications included defining "significant federal crime" to mean any federal felony and defining the term "reasonable indication" to be substantially lower than "probable cause." The memorandum also requires notification to take place without delay. The only remaining open point, albeit a significant issue, is the type of advice that the Criminal Division is permitted to provide the FBI after it has been notified of a possible criminal violation. In this regard, in March 2002, the Attorney General signed revised proposed procedures for sharing and coordinating FISA investigations, including changes resulting from the USA Patriot Act of 2001. However, the procedures must be approved by the FISA Court, which recently rejected some of the them as going too far in terms of loosening the barriers between criminal investigations and intelligence gathering.
To improve coordination between the FBI and the Criminal Division by ensuring that investigations that indicate criminal violations are clearly identified and by institutionalizing mechanisms to ensure greater coordination, we recommend that the Attorney General direct that all FBI memorandums sent to OIPR, summarizing investigations or seeking FISA renewals contain a section devoted explicitly to identifying any possible federal criminal violation meeting the Attorney General's coordination criteria, and that those memorandums of investigation meeting the criteria for Criminal Division notification be timely coordinated with the division.	Implemented. In an August 6, 2001, memorandum, the Deputy Attorney General directed the FBI to explicitly devote a section in its foreign counterintelligence case summary memorandums, which it sends to OIPR in connection with an initial FISA request or renewal, for identification of any possible federal criminal violations associated with the cases. OIPR is to make those memorandums available to the Criminal Division. The Deptuy Attorney General's memorandum also required that, when the notification standard is met, notification should be accomplished without delay.
To improve coordination between the FBI and the Criminal Division by ensuring that investigations that indicate a criminal violation are clearly identified and by institutionalizing mechanisms to ensure greater coordination, we recommend that the Attorney General direct the FBI Inspection Division, during its periodic inspections of foreign counterintelligence investigations at field offices, to review compliance with the requirement for case summary memorandums sent OIPR to specifically address the identification of possible criminal violations. Moreover, where field office case summary memorandums identified reportable instances of possible federal crimes, the Inspection Division should assess whether the appropriate headquarters unit properly coordinated those foreign counterintelligence investigations with the Criminal Division.	Implemented. In a July 18, 2001, memorandum to the Deputy Attorney General, the Assistant Director of the FBI's Inspection Division stated that the division has established a Foreign Intelligence/Counterintelligence Audit that is to be completed during its on-site inspections at applicable FBI field offices. The audit, according to the Assistant Director, will determine whether significant criminal activity was indicated during intelligence investigations and, where such activity was identified, determine whether it was properly coordinated with FBI headquarters and Justice's Criminal Division.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
To improve coordination between the FBI and the Criminal Division by ensuring that investigations that indicate criminal violations are clearly identified and by institutionalizing mechanisms to ensure greater coordination, we recommend that the Attorney General issue written policies and procedures establishing the roles and responsibilities of OIPR and the core group as mechanisms for ensuring compliance with the Attorney General's coordination procedures.	Implemented. On June 12, 2001, OIPR issued policy guidance to its staff on compliance with the Attorney General's 1995 coordination procedures. The issuance of this policy partially implements the GAO recommendation. Later on August 6, 2001, the Deputy Attorney General issued a memorandum to the Criminal Division, the FBI and OIPR establishing the roles and responsibilities of the Core Group to resolve disputes arising from the Attorney General's 1995 guidelines.

Combating Terrorism: Actions Needed To Improve DOD Antiterrorism Program Implementation and Management (GAO-01-909, Sept. 19, 2001). Recommendations pp. 26 and 27.

GAO recommendations	Status of recommendations
To improve the implementation of the DOD antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to identify those installations that serve a critical role in support of our national military strategy, and to ensure that they receive a higher headquarters vulnerability assessment regardless of the number of personnel assigned at the installations.	Partially implemented. DOD is in the process of changing its antiterrorism standards.
To improve the implementation of the DOD antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to develop a strategy to complete higher headquarters vulnerability assessments at National Guard installations.	Partially implemented. DOD 's primary action officer is working with Army and Air National Guard to provide vulnerability assessments.
To improve the implementation of the DOD antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to clarify the force protection standard requiring a criticality assessment at each installation to specifically describe the factors to be used in the assessment and how these evaluations should support antiterrorism resource priority decisions.	Partially implemented. DOD is in the process of updating its antiterrorism handbook.
To improve the implementation of the DOD antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to expand the threat assessment methodology to increase awareness of the consequences of changing business practices at installations that may create workplace violence situations or new opportunities for individuals not affiliated with DOD to gain access to installations.	Implemented. DOD has reviewed its threat methodology to ensure that no threat indicators are ignored or overlooked.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
To improve the implementation of the DOD antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to require each installation commander to form a threat working group and personally and actively engage state, local, and federal law enforcement officials. These working groups should hold periodic meetings, prepare records of their discussions, and provide threat information to installation commanders regularly.	Partially implemented. DOD is in the process of updating its antiterrorism handbook.
To strengthen management of the antiterrorism program, we recommend that the Secretary of Defense direct the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to establish a management framework for the antiterrorism program that would provide the department with a vehicle to guide resource allocations and measure the results of improvement efforts. This framework should include A strategic plan that defines • long-term antiterrorism goals, • approaches to achieve the goals, and • key factors that might significantly affect achieving the goals, and An implementation plan that describes • performance goals that are objective, quantifiable, and measurable, and resources to achieve the goals; • performance indicators to measure outputs; • an evaluation plan to compare program results to established goals; and • actions needed to address any unmet goals.	Partially implemented. DOD is planning to issue a management plan to include the elements of GAO's recommendation.

Combating Terrorism: Selected Challenges and Related Recommendations (GAO-01-822, Sept. 20, 2001). Recommendations pp. 41, 42, 57, 86, 87, 104, and 128.

GAO recommendations	Status of recommendations
We recommend that the President, in conjunction with the Vice President's efforts, appoint a single focal point that has the responsibility and authority for all critical leadership and coordination functions to combat terrorism.	Implemented. Through Executive Order (EO) 13228, the President established an Office of Homeland Security (OHS) to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.
• The focal point should be in the Executive Office of the President, outside individual agencies, and encompass activities to include prevention, crisis management, and consequence management.	Implemented. EO 13228 establishes OHS within the Executive Office of the President. OHS functions include efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
• The focal point should oversee a national-level authoritative threat and risk assessment on the potential use of WMD by terrorists on U.S. soil. Such assessments should be updated regularly.	Partially implemented. EO 13228 states that OHS shall identify priorities and coordinate efforts for collection and analysis of information within the United States regarding threats of terrorism against the United States and activities of terrorists or terrorist groups within the United States. OHS shall identify, in coordination with NSC, priorities for collection of intelligence outside the United States regarding threats of terrorism within the United States. EO 13228 does not address risk assessments.
• The focal point also should lead the development of a national strategy for combating terrorism.	Implemented. EO 13228 states that OHS will develop a comprehensive national strategy to secure the United States from terrorist threats or attacks. The National Strategy for Homeland Security was issued in July 2002.
• The national strategy should include (1) desired outcomes that can be measured and are consistent with the Results Act, (2) state and local government input to better define their roles in combating terrorism, and (3) research and development priorities and needs in order to facilitate interagency coordination, decrease duplication, and leverage monetary resources.	Partially implemented. (1) The National Strategy for Homeland Security, while not including measurable outcomes, calls for their development. (2) OHS worked with state and local governments to develop the national strategy. (3) The National Strategy for Homeland Security includes a discussion of research and development.
• The focal point should coordinate implementation of the national strategy among the various federal agencies. This would entail reviewing agency and interagency programs to ensure that they are being implemented in accordance with the national strategy and do not constitute duplication of effort.	Partially implemented. EO 13228 directs OHS to coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. OHS shall work with, among others, federal agencies to ensure the adequacy of the national strategy for detecting, preparing for, preventing, protecting against, responding to, and recovering from terrorist attacks within the United States and shall periodically review and coordinate revisions to that strategy as necessary. The National Strategy for Homeland Security was issued in July 2002. Given the recent publication of the plan, it is too early to determine the OHS role in coordinating its implementation.
• The focal point should analyze and prioritize governmentwide budgets and spending to combat terrorism to eliminate gaps and duplication of effort. The focal point's role will be to provide advice or to certify that the budgets are consistent with the national strategy, not to make final budget decisions.	Implemented. EO 13228 states OHS shall work with OMB and agencies to identify homeland security programs, and shall review and provide advice to OMB and departments and agencies for such programs. Per EO 13228, OHS shall certify that the funding levels are necessary and appropriate for the homeland security-related activities of the executive branch.
• The focal point should coordinate the nation's strategy for combating terrorism with efforts to prevent, detect, and respond to computer-based attacks on critical infrastructures. We do not see the focal point for combating terrorism also having responsibility for protecting computer-based infrastructures because the threats are broader than terrorism and such programs are more closely associated with traditional information security activities. Nonetheless, there should be close coordination between the two areas.	Implemented. Per EO 13228, OHS shall coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. In performing this function, the office shall work with federal, state, and local agencies, and private entities as appropriate to, among other things, coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attacks. In addition, the President created a Special Advisor for Cyberspace Security and appointed him as Chair of the President's Critical Infrastructure Protection Board. This Chair reports to both OHS and NSC.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
• The focal point should be established by legislation to provide it with legitimacy and authority, and its head should be appointed by the President with the advice and consent of the U.S. Senate. This would provide accountability to both the President and Congress. Also, it would provide continuity across administrations.	Not implemented. However, there have been bills before Congress that would legislatively create a central focal point (e.g., OHS), making its director subject to appointment with the advice and consent of the U.S. Senate.
• The focal point should be adequately staffed to carry out its duties for planning and oversight across the federal government.	Partially implemented. EO 13228 has provisions for OHS to hire staff, and for other federal departments to detail their staff to OHS. Given the relative newness of OHS, it is too early to determine whether staff levels are adequate.
• The focal point should develop a formal process to capture and evaluate interagency lessons learned from major interagency and intergovernmental federal exercises to combat terrorism. The focal point should analyze interagency lessons learned and task individual agencies to take corrective actions as appropriate.	Partially implemented. Per EO 13228, OHS shall coordinate domestic exercises and simulations designed to assess and practice systems that would be called upon to respond to a terrorist threat or attack within the United States and coordinate programs and activities for training. OHS shall also ensure that such programs and activities are regularly evaluated under appropriate standards and that resources are allocated to improving and sustaining preparedness based on such evaluations. Given the relative newness of OHS, it is too early to determine how it has implemented this responsibility.
To help support a national strategy, we recommend that the Attorney General direct the Director of the FBI to work with appropriate agencies across government to complete ongoing national-level threat assessments regarding terrorist use of WMD.	Partially implemented. The Department of Justice and the FBI agreed to this recommendation. According to the FBI, it is currently working on a comprehensive national-level assessment of the terrorist threat to the U.S. homeland. The FBI said that this will include an evaluation of the chemical and biological weapons most likely to be used by terrorists and a comprehensive analysis of the risks of terrorists using other WMD. The FBI estimates the assessment will be completed in November 2002.
To guide federal efforts in combating domestic terrorism, we recommend that the Attorney General use the Five-Year Interagency Counterterrorism and Technology Crime Plan and similar plans of other agencies as a basis for developing a national strategy by including (1) desired outcomes that can be measured and that are consistent with the Results Act and (2) state and local government input to better define their roles in combating terrorism.	Partially implemented. The Department of Justice asserted that the Five-Year Plan included desired outcomes. We disagreed with the department and believed what it cited as outcomes are outputs—agency activities rather than results the federal government is trying to achieve. The National Strategy for Homeland Security, issued in July 2002, supercedes the Attorney General's Five-Year Plan as the interagency plan for combating terrorism domestically. This strategy does not include measurable outcomes, but calls for their development.
To improve readiness in consequence management, we recommend that the Director of FEMA play a larger role in managing federal exercises to combat terrorism. As part of this, FEMA should seek a formal role as a cochair of the Interagency Working Group on Exercises and help to plan and conduct major interagency counterterrorist exercises to ensure that consequence management is adequately addressed.	FEMA agreed with the recommendation. GAO is working with FEMA to determine the status of implementation. In June 2002, the President proposed that a new Department of Homeland Security take the lead for developing and conducting federal exercises to combat terrorism.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
To ensure that agencies benefit fully from exercises in which they participate, we recommend that the Secretaries of Agriculture, Defense, Energy, Health and Human Services, and Veterans Affairs; the Directors of the Bureau of Alcohol, Tobacco, and Firearms, FEMA, FBI, and the U.S. Secret Service; the Administrator of the Environmental Protection Agency; and the Commandant of the U.S. Coast Guard require their agencies to prepare after-action reports or similar evaluations for all exercises they lead and for all field exercises in which they participate.	Partially implemented. Several of the agencies agreed with this recommendation and cited steps they were taking to ensure that after-action reports or similar evaluations are completed as appropriate for exercises to combat terrorism. For example, DOD has used its Joint Uniform Lessons Learned System to document observations and lessons learned during exercises, including interagency exercises to combat terrorism. Other agencies taking steps to improve their evaluations of exercises include the Department of Energy and the FBI.
To reduce duplication and leverage resources, we recommend that the Assistant to the President for Science and Technology complete efforts to develop a strategic plan for research and development to combat terrorism, coordinating this with federal agencies and state and local authorities.	Partially implemented. The National Strategy for Homeland Security includes a chapter on science and technology, which includes an initiative to coordinate research and development of the homeland security apparatus. The proposed Department of Homeland Security, working with the White House and other federal departments, would set the overall direction for homeland security research and development. The proposed department would also establish a network of national laboratories for homeland security. Given that the department is only a proposal at this time, it is too early to determine how it might implement our recommendation.
To eliminate overlapping assistance programs and to provide a single liaison for state and local officials, we recommend that the President, working closely with Congress, consolidate the activities of the FBI's National Domestic Preparedness Office and the Department of Justice's Office for State and Local Domestic Preparedness Support under FEMA.	Partially implemented. In June 2002, the President proposed that a new Department of Homeland Security take the lead for federal programs to assist state and local governments. Given that the department is only a proposal at this time, it is too early to determine whether these offices and their functions have been successfully consolidated.
To clarify the roles and missions of specialized National Guard response teams in a terrorist incident involving WMD, we recommend that the Secretary of Defense suspend the establishment of any additional National Guard Weapons of Mass Destruction Civil Support Teams until DOD has completed its coordination of the teams' roles and missions with the FBI. We also recommend that the Secretary of Defense reach a written agreement with the Director of the FBI that clarifies the roles of the teams in relation to the FBI.	Partially implemented. Subsequent to our earlier report on these teams, and a report by the DOD Inspector General, which found some similar problems, DOD agreed to review the National Guard teams and work with other agencies to clarify their roles in responding to terrorist incidents. In September 2001, DOD restricted the number of teams to 32.

(Continued From Previous Page)

GAO recommendations	Status of recommendations
To strengthen the federal government's critical infrastructure strategy, we recommend that the Assistant to the President for National Security Affairs define • specific roles and responsibilities of organizations involved in critical infrastructure protection and related information security activities; • interim objectives and milestones for achieving CIP goals and a specific action plan for achieving these objectives, including implementation of vulnerability assessments and related remedial plans; and • performance measures for which entities can be held accountable.	Not implemented: The President's Critical Infrastructure Protection Board released a draft strategy on September 18, 2002, for comment. The draft does not specify roles and responsibilities, or performance measures. However, the President's Critical Infrastructure Protection Board plans to periodically update the strategy as it evolves. The draft also states that other groups have developed strategies related to their portion of cyberspace they own or operate. Further, the President's national strategy for homeland security, issued in July 2002, states that a comprehensive national infrastructures plan will be issued in the future.
We believe the federal government's cyber-security strategy should be linked to the national strategy to combat terrorism. However, the two areas are different in that the threats to computer-based infrastructures are broader than terrorism and programs to protect them are more closely associated with traditional information security activities.	Regarding the link with efforts to combat terrorism, the draft strategy states that it supports both the National Strategy for Homeland Security and the National Security Strategy of the United States.

Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains (GAO-02-610, June 7, 2002).
Recommendations, p. 20.

GAO recommendations	Status of recommendations
We recommend that the President direct OHS to (1) develop a comprehensive, governmentwide definition of homeland security, and (2) include the definition in the forthcoming national strategy.	Implemented. In July 2002, OHS published the National Strategy for Homeland Security. In this document, there is a detailed definition of homeland security.

Nonproliferation R&D: NNSA's Program Develops Successful Technologies, but Project Management Can Be Strengthened (GAO-02-904, Aug. 23, 2002). Recommendations, pp. 20-21.

GAO recommendations	Status of recommendations
We recommend that the Administrator of the National Nuclear Security Administration (NNSA) work with OHS (or the Department of Homeland Security, if established) to clarify the Nonproliferation and Verification Research and Development Program's role in relation to other agencies conducting counterterrorism research and development and to achieve an appropriate balance between short-term and long-term research. In addition, to improve the program's ability to successfully transfer new technologies to users, the program should, in cooperation with OHS, allow users opportunities to provide input through all phases of research and development projects	Partially implemented. NNSA agreed to the recommendation and stated that it will improve coordination with other agencies conducting research and development. In addition, coordination may be improved if two of the program's divisions are moved to a new Department of Homeland Security, as proposed by the President.

Related GAO Products

Homeland Security

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

National Preparedness: Technology and Information Sharing Challenges. GAO-02-1048R. Washington, D.C.: August 30, 2002.

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

Homeland Security: Effective Intergovernmental Coordination is Key to Success. GAO-02-1012T. Washington, D.C.: August 22, 2002.

Homeland Security: Effective Intergovernmental Coordination Is Key to Success. GAO-02-1011T. Washington, D.C.: August 20, 2002.

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

Chemical Safety: Emergency Response Community Views on the Adequacy of Federally Required Chemical Information. GAO-02-799. Washington, D.C.: July 31, 2002.

*Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenge*s. GAO-02-971T. Washington, D.C.: July 25, 2002.

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

Homeland Security: Critical Design and Implementation Issues. GAO-02-957T. Washington, D.C.: July 17, 2002.

Homeland Security: New Department Could Improve Coordination but Transferring Control of Certain Public Health Programs Raises Concerns. GAO-02-954T. Washington, D.C.: July 16, 2002.

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

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

Homeland Security: New Department Could Improve Biomedical R&D Coordination but May Disrupt Dual-Purpose Efforts. GAO-02-924T. Washington, D.C.: July 9, 2002.

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

Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success. GAO-02-901T. Washington, D.C.: July 3, 2002.

Homeland Security: New Department Could Improve Coordination but May Complicate Priority Setting. GAO-02-893T. Washington, D.C.: June 28, 2002.

Homeland Security: New Department Could Improve Coordination but May Complicate Public Health Priority Setting. GAO-02-883T. Washington, D.C.: June 25, 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.

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

Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains. GAO-02-610. Washington, D.C.: June 7, 2002.

National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy. GAO-02-811T. Washington, D.C.: June 7, 2002.

Review of Studies of the Economic Impact of the September 11, 2001, Terrorist Attacks on the World Trade Center. GAO-02-700R. Washington, D.C.: May 29, 2002.

Homeland Security: 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.

Homeland Security: Progress Made, More Direction and Partnership Sought. GAO-02-490T. Washington, D.C.: March 12, 2002.

Homeland Security: Challenges and Strategies in Addressing Short- and Long-Term National Needs. GAO-02-160T. Washington, D.C.: November 7, 2001.

Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts. GAO-02-208T. Washington, D.C.: October 31, 2001.

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

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

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

Combating Terrorism

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

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

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

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

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

Nuclear Nonproliferation: U.S. Efforts to Combat Nuclear Smuggling. GAO-02-989T. Washington, D.C.: July 30, 2002.

Combating Terrorism: Preliminary Observations on Weaknesses in Force Protection for DOD Deployments Through Domestic Seaports. GAO-02-955TNI. Washington, D.C.: July 23, 2002.

Diffuse Security Threats: Technologies for Mail Sanitization Exist, but Challenges Remain. GAO-02-365. Washington, D.C.: April 23, 2002.

Combating Terrorism: Intergovernmental Cooperation in the Development of a National Strategy to Enhance State and Local Preparedness. GAO-02-550T. Washington, D.C.: April 2, 2002.

Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy. GAO-02-549T. Washington, D.C.: March 28, 2002.

Combating Terrorism: Critical Components of a National Strategy to Enhance State and Local Preparedness. GAO-02-548T. Washington, D.C.: March 25, 2002.

Combating Terrorism: Intergovernmental Partnership in a National Strategy to Enhance State and Local Preparedness. GAO-02-547T. Washington, D.C.: March 22, 2002.

Combating Terrorism: Key Aspects of a National Strategy to Enhance State and Local Preparedness. GAO-02-473T. Washington, D.C.: March 1, 2002.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Public Health

Public Health: Maintaining an Adequate Blood Supply Is Key to Emergency Preparedness. GAO-02-1095T. Washington, D.C.: September 10, 2002.

Homeland Security: New Department Could Improve Coordination But May Complicate Public Health Priority Setting. GAO-02-883T. Washington, D.C.: June 25, 2002.

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

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

Bioterrorism: Public Health and Medical Preparedness. GAO-02-141T. Washington, D.C.: October 10, 2001.

Bioterrorism: Coordination and Preparedness. GAO-02-129T. Washington, D.C.: October 5, 2001.

Bioterrorism: Federal Research and Preparedness Activities. GAO-01-915. Washington, D.C.: September 28, 2001.

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

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

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

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

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

Disaster Assistance

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

FEMA and Army Must Be Proactive in Preparing States for Emergencies. GAO-01-850. Washington, D.C.: August 13, 2001.

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

Budget and Management

Performance Budgeting: Opportunities and Challenges. GAO-02-1106T. Washington, D.C.: September 19, 2002.

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

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

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

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

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

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

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

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

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

Managing for Results: Federal Managers' Views on Key Management Issues Vary Widely across Agencies. GAO-01-0592. Washington, D.C.: May 2001.

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

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

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

Grant Design

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

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

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