

August 2003

HOMELAND
SECURITY

Efforts to Improve
Information Sharing
Need to Be
Strengthened



G A O

Accountability * Integrity * Reliability



Highlights of GAO-03-760, a report to the Secretary of Homeland Security

HOMELAND SECURITY

Efforts to Improve Information Sharing Need to Be Strengthened

Why GAO Did This Study

The sharing of information by federal authorities to state and city governments is critical to effectively execute and unify homeland security efforts. This report examines (1) what initiatives have been undertaken to improve information sharing and (2) whether federal, state, and city officials believe that the current information-sharing process is effective.

What GAO Recommends

We recommend that the Secretary of Homeland Security work with the heads of other federal agencies, and state and city officials to ensure that DHS's enterprise architecture fully integrates states and cities into the information-sharing process; incorporates, where appropriate, other federal, state, and city information-sharing initiatives; takes specific actions to evaluate and overcome perceived barriers to information sharing; and measure progress in improving information sharing as part of the enterprise architecture initiative.

The Departments of Homeland Security and Defense concurred with our report. DHS stated that it has made improvements in information sharing but further progress will require a prudent and deliberate approach. The Central Intelligence Agency provided only technical comments. The Department of Justice did not agree with our findings. However, we believe that our conclusions are well founded.

www.gao.gov/cgi-bin/getrpt?GAO-03-760.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Raymond J. Decker at (202) 512-6020 or deckerrj@gao.gov.

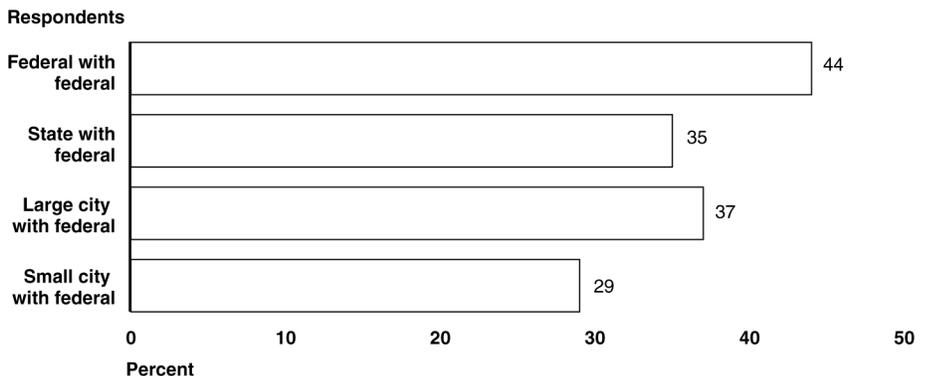
What GAO Found

Since September 11, 2001, federal, state, and city governments have established initiatives to improve the sharing of information to prevent terrorism. Many of these initiatives were implemented by states and cities and not necessarily coordinated with other sharing initiatives, including those by federal agencies. At the same time, the Department of Homeland Security (DHS) has initiatives under way to enhance information sharing, including the development of a homeland security blueprint, known as an "enterprise architecture," to integrate sharing between federal, state, and city authorities.

GAO surveyed federal, state, and city government officials on their perceptions of the effectiveness of the current information-sharing process. Numerous studies, testimonies, reports, and congressional commissions substantiate our survey results. Overall, no level of government perceived the process as effective, particularly when sharing information with federal agencies. Information on threats, methods, and techniques of terrorists is not routinely shared; and the information that is shared is not perceived as timely, accurate, or relevant. Moreover, federal officials have not yet established comprehensive processes and procedures to promote sharing. Federal respondents cited the inability of state and city officials to secure and protect classified information, the lack of federal security clearances, and a lack of integrated databases as restricting their ability to share information.

DHS needs to strengthen efforts to improve the information sharing process so that the nation's ability to detect or prepare for attacks is strengthened.

Agencies Responding to Our Survey and Indicating That Information Sharing with Federal Agencies Is Effective or Very Effective



Source: GAO.

Contents

Letter		1
	Results in Brief	3
	Background	6
	Information-Sharing Initiatives Are Not Well Coordinated	11
	Current Information-Sharing Process Not Perceived As Effective	15
	Conclusions	29
	Recommendations for Executive Action	30
	Agency Comments and Our Evaluation	31
Appendix I	Scope and Methodology	35
	Use of a Survey to Supplement Interviews and Review of Documents	36
Appendix II	Selected Initiatives to Promote Information Sharing	38
Appendix III	Survey Responses Showing Categories of Homeland Security Information Deemed Needed by the Respondents	40
Appendix IV	Survey Responses to Our Questions on the Elements of an Information-Sharing Process That Are Already in Place	42
Appendix V	Survey Responses to Perceived Barriers Faced by States/Cities in Providing the Federal Government with Information	44
Appendix VI	Comments from the Department of Homeland Security	45

Appendix VII	Comments from the Department of Defense	47
Appendix VIII	Comments from the Department of Justice	50
Appendix IX	GAO Contacts and Staff Acknowledgments	52
Related GAO Products		53

Tables

Table 1: GAO Surveys Distributed, Survey Responses, and Response Rates	2
Table 2: Percentage of Federal, State, and City Respondents That View Their Sharing Relationships with One Another As Effective or Very Effective	18
Table 3: Perceptions of Information Needed and Regularly Received	20
Table 4: Survey Respondents Who Said the Information from the Federal Government Was Timely, Accurate, or Relevant	23
Table 5: Survey Respondents Who Said That Information from State Agencies Was Timely, Accurate, or Relevant	24
Table 6: Survey Respondents Who Said That Information from City Agencies Was Timely, Accurate, or Relevant	25
Table 7: Perceived Barriers Preventing Federal Agencies from Providing Other Federal Agencies, States, and Cities with Information	27
Table 8: Initiatives and Efforts to Share More Information	38
Table 9: Needed to Critically-Needed Information and Intelligence and Frequently to Regularly-Received Information and Intelligence	40
Table 10: Survey Respondents Who Agreed That Elements of a Sharing Framework Exists by Answering “Great” to “Very Great”	42
Table 11: Great to Very-Great Barriers to Providing Federal Authorities with Information and Intelligence	44

Abbreviations

CATIC	California Anti-Terrorism Information Center
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
JITF-CT	Joint Intelligence Task Force-Combating Terrorism
JRIES	JITF-CT/RISS.NET Information Exchange System
JTTF	Joint Terrorism Task Force
MDA	Maritime Domain Awareness
SATURN	Statewide Anti-Terrorism Unified Response Network

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States General Accounting Office
Washington, DC 20548

August 27, 2003

The Honorable Thomas J. Ridge
The Secretary of Homeland Security

Dear Mr. Secretary:

Information—its timely collection, thorough analysis, and appropriate dissemination—is critical to unifying the efforts of federal, state, and local government agencies in preventing terrorist attacks. For this report, our objectives were to determine (1) what initiatives have been undertaken to improve information sharing and (2) whether federal, state, and city officials believe that the current information-sharing process is effective. To meet these objectives, we gathered information on national planning efforts and obtained the perceptions of federal, state, and city governments on how the current information-sharing process was working.

Specifically, we met with officials who were knowledgeable about information sharing from federal, state, and city agencies and officials from associations representing cities, police organizations, and research groups. Our scope focused on the information-sharing process between federal, state, and city governments. We did not include county governments or the private sector (which owns more than 80 percent of the nation's critical infrastructure), although we recognize that both have important roles in homeland security. We also did not include the federal government's critical infrastructure protection efforts, for which GAO has made numerous recommendations over the last several years. Additionally, most of our fieldwork was performed before the Department of Homeland Security (DHS) began operations in January 2003. Thus, some of the federal agencies we worked with were still part of other cabinet departments at the time of our research. Additionally, the department's efforts to establish a homeland security blueprint—referred

to as its “enterprise architecture”¹—are in the early stages of development. We also reviewed relevant reports, testimonies, and position papers.

Additionally, to supplement this analysis, we conducted a survey of officials representing the federal intelligence community and law enforcement agencies; state homeland security offices; all cities with a population of 100,000 or more; and a sample of cities with a population between 50,000 and 100,000, to obtain their perceptions about the current information-sharing process. We did not independently validate that the perceptions reported in our survey, such as the types of information that respondents said they needed, accurately represent the condition of the information-sharing process. However, our survey results typically corroborated the condition of the current information-sharing process that was described in our interviews with knowledgeable officials and in our review of documents. Eighty percent, or 40 of the 50 state homeland security advisors, completed the survey. Our overall response rate for the survey was 50 percent and represents 284 government entities. Table 1 summarizes the number of surveys distributed and the response rates for the federal, state, and city respondents.

Table 1: GAO Surveys Distributed, Survey Responses, and Response Rates

	Federal intelligence and law enforcement agencies	State homeland security advisors	Cities		Totals
			Population of over 100,000	Population of under 100,000 ^a	
Number of surveys	29	50	242	243	564
Number of responses	16	40	106	122	284
Response rate in percents	55%	80%	44%	50%	50%

Source: GAO.

Note: Although our results represent a substantial number of governmental entities, the results do not represent the entire population of governmental entities involved in information sharing.

^aCities with a population of between 50,000 and 100,000 were selected by random sample.

¹ An enterprise architecture can be viewed as a blueprint that describes an entity’s operational and technical environments. The blueprint includes descriptive models of the entity’s current and future business and technical environments, along with a roadmap for transitioning from the current to the future environment.

We conducted our review from June 2002 through May 2003 in accordance with generally accepted government auditing standards. A complete discussion of our scope and methodology is contained in appendix I.

Results in Brief

Federal agencies and state and city governments have undertaken initiatives to improve the sharing of information that could be used to fight terrorism and protect the homeland. Many of the initiatives were implemented by states and cities and are not necessarily coordinated with other sharing initiatives, including those implemented by the federal government. Recognizing that information sharing to fight terrorism is a key factor in homeland security, the U.S. Department of Homeland Security has a number of initiatives under way to enhance information-sharing, including the development of a homeland security blueprint, referred to as an enterprise architecture. Through this architecture, DHS plans to integrate the sharing of information within the federal government and between federal agencies, state and city governments, and the private sector. According to DHS, the department plans to issue the enterprise architecture in September 2003 and begin implementation in November 2003.

Recent legislation and various national strategies specify actions to improve the sharing of information that could be used to fight terrorism. For example, the Homeland Security Act of 2002² requires DHS to coordinate homeland security information sharing with nonfederal entities, including state and local government personnel, and requires the President of the United States to prescribe and implement procedures, issued July 29, 2003, under which federal agencies share homeland security information with other federal agencies and appropriate state and local government personnel.³ The July 2002 *National Strategy for Homeland Security*⁴ and the February 2003 *National Strategy for the*

² Public Law 107-296, enacted Nov. 25, 2002.

³ The President has assigned responsibility for this function to the Secretary of Homeland Security. Executive Order 13311, *Homeland Security Information Sharing*, July 29, 2003.

⁴ Office of the President, *The National Strategy for Homeland Security* (Washington, D.C.: July 2002).

*Physical Protection of Critical Infrastructures and Key Assets*⁵ also call for actions to improve information sharing.

In the meantime, without this overall coordination, some federal, state, and city entities have implemented their own information-sharing initiatives. For example, the Federal Bureau of Investigation (FBI) has significantly increased the number of its Joint Terrorism Task Forces. Also, California established an antiterrorism information center that collects, analyzes, and disseminates information to its law enforcement officers, other law enforcement agencies, and FBI. In our survey, 34 of 40 states and 160 of 228 cities stated that they participate in information-sharing centers. While these initiatives may increase the sharing of information to fight terrorism, they are not well coordinated and consequently risk creating partnerships that may actually limit some participants' access to information and duplicating efforts of some key agencies in each level of government. Moreover, while beneficial to these participants, the initiatives do not necessarily integrate others into a truly national system and may inadvertently hamper information sharing for this reason. A lack of effective integration could increase the risk that officials will overlook, or never even receive, information needed to prevent a terrorist attack.

Despite various legislation, strategies, and initiatives to improve information sharing, the documents we reviewed and officials we interviewed from federal agencies, states, and cities and those that responded to our survey generally do not consider the current process of sharing information to protect the homeland to be effective. For example, only 13 percent of federal government respondents reported that sharing information with states and cities was "effective" or "very effective." And, of the 40 states that responded, only 35 percent reported that sharing with the federal government was "effective" or "very effective."

The three levels of government identified three main systemic problems that account for this perception. First, no level of government was satisfied that they receive enough information. In general, survey respondents reported that they are typically receiving less than 50 percent of specified categories of information that they perceive they need to

⁵ Office of the President, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: February 2003).

support their homeland security duties. For example, 98 percent of the large cities that completed our survey reported that they needed information on the movement of known terrorists; however, only 15 percent reported that they received this information. Second, no level of government was satisfied with the timeliness, accuracy, or relevance of the information they received. States and cities reported that threat information received is often untimely, inaccurate, or irrelevant. Third, the federal government still perceives the fight against terrorism, particularly its prevention, to be generally a federal responsibility, which potentially undermines the unity of effort between federal, state, and city governments needed to effectively secure the homeland. Consequently, the federal government still has not established comprehensive policies or procedures to effectively integrate state and city governments into the information-sharing process or even routinely recognize their role in this process. For example, 30 of 40 states and 212 of 228 cities responding to our survey reported that they were not given the opportunity to participate in national policy making on information sharing. As a result, opportunities are routinely missed to engage state and city law enforcement officers in obtaining and providing the federal government with information that could be vital in the war against terrorism.

The federal agencies in our survey identified several barriers to sharing threat information with state and city governments. On the other hand, state and city governments did not perceive that the barriers identified by the federal agencies were truly barriers.⁶ According to our survey, when federal agencies felt they could not provide states and cities with information, they cited concerns over state and local officials' ability to secure and protect classified information, the officials' lack of security clearances, and the lack of integrated databases. However, we believe that these perceived barriers could be overcome. For example, state and local police agencies routinely handle and protect "law enforcement sensitive" information to build cases against suspected criminals, suggesting that—with proper training and equipment—these government agencies could handle other categories of sensitive information. An information-sharing process in which needed information is not routinely received or is received but is untimely or irrelevant hampers the nation's collective ability to effectively unify the efforts of all levels of government. An unwillingness to share information because of a perception that

⁶ The federal government perceived that more barriers exist to providing states and cities with information than states and cities perceived.

barriers prevent sharing further affects information, collection, analysis, and dissemination at each level of government charged with homeland security.

We are recommending that the Secretary of Homeland Security, in developing the enterprise architecture, (1) work in conjunction with the heads of other federal agencies, state and city authorities, and the private sector to ensure that the department's enterprise architecture fully integrates them into the information-sharing process and (2) take specific actions, including obtaining the private sector's views regarding information sharing, to evaluate and overcome the perceived barriers that prevent information sharing today. In commenting on a draft of this report, the Departments of Defense and Homeland Security concurred with our report, and the latter indicated that it has made improvements to information sharing but that further progress will require a prudent and deliberate approach. The Department of Justice did not concur with our report and questioned the reliability of our evidence. However, we used evidence from a variety of sources including well-respected research organizations, testimony before committees of the Congress, interviews with intelligence or law enforcement officers at all levels of government, and our survey, and consider this evidence to be reliable and our conclusions well founded.

Background

A constitutional role of the federal government is to provide for the common defense, which includes preventing terrorist attacks. The government must prevent and deter attacks on our homeland as well as detect impending danger before attacks occur. Although it may be impossible to detect, prevent, or deter every attack, steps can be taken to reduce the risk posed by the threats to homeland security. Traditionally, protecting the homeland against these threats was generally considered a federal responsibility. To meet this responsibility, the federal government gathers intelligence, which is often classified as national security information. This information is protected and safeguarded to prevent unauthorized access by requiring appropriate security clearances and a "need to know." Generally, the federal government did not share national level intelligence with states and cities, since they were not viewed as having a significant role in preventing terrorism. Therefore, the federal government did not generally grant state and city officials access to classified information. However, as we reported in June 2002, the view that states and cities do not have a significant role in homeland security has changed since September 11, 2001, and the need to coordinate the

efforts of federal, state, and local governments for homeland security is now well understood.⁷

Preventing Terrorism Has Traditionally Been Viewed As a Federal Responsibility

Protecting the United States from terrorism has traditionally been a responsibility of the federal government and, typically, the views of states and cities in formulating national policy have not been considered. In the Homeland Security Act of 2002, Congress found that the federal government relies on state and local personnel to protect against terrorist attacks and that homeland security information is needed by state and local personnel to prevent and prepare for such attacks. Congress also found that federal, state, and local governments; and intelligence, law enforcement, and other emergency and response personnel must act in partnership to maximize the benefits of information gathering and analysis to prevent and respond to terrorist attacks. As a result, the act expressed the sense of Congress that federal, state, and local entities should share homeland security information to the maximum extent practicable. Federal, state, and local governments and the private sector were not fully integrated participants before the September 11, 2001, attacks, but the need to integrate them became more widely recognized afterward.

In order to develop national policies and strategies to address terrorism issues, senior policymakers obtain information from the intelligence community.⁸ The intelligence community uses a cyclic process for intelligence production. Simplified, the intelligence community (1) receives information requirements from policymakers, (2) collects and analyzes the information from its sources, (3) creates intelligence products from the information, (4) disseminates the products to

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

⁸ The intelligence community consists of the Office of the Director of Central Intelligence (who is also the head of the intelligence community); the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Imagery and Mapping Agency; the National Reconnaissance Office; other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the Army, Navy, Marine Corps, and Air Force, the Federal Bureau of Investigation, the Department of the Treasury, the Department of Energy, and the Coast Guard; the Bureau of Intelligence and Research of the Department of State, the elements of the Department of Homeland Security concerned with the analyses of foreign intelligence information; and such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of Central Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

consumers of intelligence, and (5) receives feedback about the usefulness of the information from consumers. This process can lead to additional information requirements and is ongoing.

Since the late 1940s, the federal government generally separated law enforcement and intelligence functions, although both have a role in combating terrorism.⁹ From this separation, law enforcement and intelligence were created and handled differently, depending on which community obtained the information and how it was to be used. The law enforcement community investigates criminal activity and supports prosecutions by providing information related to events that have occurred. In contrast, the intelligence community tries to provide policymakers and military leaders with information so that decisions can be made to protect and advance national interests. Often, the intelligence community collects information from sensitive sources or using special methods and keeps the information classified to protect their sources and methods and ensure a continual flow in the future.

Executive Order no. 12958, Classified National Security Information, as amended, prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information related to defense against transnational terrorism. Executive Order no. 12968, Access to Classified Information, states that access to classified national security information is generally limited to persons who have been granted a security clearance, been briefed as to their responsibilities for protecting classified national security information, have signed a nondisclosure agreement acknowledging those responsibilities, and have agreed to abide by all appropriate security requirements. In addition, these persons must have a demonstrated “need to know” the information in connection with the performance of their official functions. If these criteria are not met, then the information is not to be shared.

The federal intelligence community has traditionally not always considered states or cities to need access to intelligence that could be used to fight terrorism. As a result, few officials at the state and local levels have the clearances required for access to intelligence products.

⁹ The National Security Act of 1947 prohibited the Central Intelligence Agency from having police, subpoena, law enforcement powers, or internal security functions. The intention of the law was to hold intelligence separate and distinct from law enforcement activities. The investigations of improper domestic intelligence gathering in the 1970s led to further delineation of the separation between intelligence and law enforcement functions.

Furthermore, the collection and use of intelligence information on individuals for domestic law enforcement purposes is constrained by the application of constitutional protections, statutory controls, and rules of evidence. For example, the Foreign Intelligence Surveillance Act of 1978¹⁰ had, in effect, been interpreted as requiring some separation that limited coordination between domestic law enforcement and foreign intelligence investigations, particularly with regard to the use of information collected for foreign intelligence purposes in criminal prosecutions.

September 11, 2001, Attacks Redefined Terrorism Responsibilities

Although previous terrorist attacks—such as the 1993 World Trade Center bombing—proved that the United States was not immune to attacks on its homeland, the enormity of the loss of life and impact of the terrorist attacks on September 11, 2001, highlighted the increasing risk of terrorist attacks on U.S. soil. Consequently, federal, state, and city governments recognized an urgent need to effectively unify their efforts to enhance homeland security by employing the unique contribution that each level of government can make on the basis of its capabilities and knowledge of its own environment. After the September 11, 2001, attacks, policymakers questioned the separation between law enforcement and intelligence, noting that the distinctions may limit access to some information needed to effectively execute homeland security duties. In October 2001, Congress passed the USA PATRIOT Act,¹¹ to improve the sharing of information between the intelligence and law enforcement communities, such as by providing federal investigators with more flexibility in sharing information obtained under the authority of the Foreign Intelligence Surveillance Act. In October 2002, the Senate Select Committee on Intelligence: Joint Investigation inquiry into the attacks found problems in maximizing the flow of relevant information both within the Intelligence Community as well as to and from those outside the community.¹² The review found that the reasons for these information disconnects can be, depending on the case, cultural, organizational, human, or technological. The committee

¹⁰ Public Law 95-511 (codified, as amended, at 50 U.S.C. §§ 1801-1811, 1821-1829, 1841-1846, 1861-63).

¹¹ Public Law 107-56 (enacted Oct. 26, 2001), the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001.

¹² “Counterterrorism Information Sharing with Other Federal Agencies, and with State and Local Governments and the Private Sector.” Testimony before the Select Committee on Intelligence, U.S. Senate: Joint Investigation, by Eleanor Hill, Director, Joint Inquiry Staff, Oct. 1, 2002.

recommended that comprehensive solutions, while perhaps difficult and costly, must be developed and implemented if we are to maximize our potential for success in the war against terrorism.

At the same time, recognizing a need to balance the protection of information with the emerging homeland security requirements of those that had a newly recognized need-to-know, Congress passed the Homeland Security Act of 2002 to, among other purposes, specifically facilitate information sharing. In creating the Department of Homeland Security, the act gives the Secretary the responsibility to coordinate with other executive agencies, state and local governments, and the private sector in order to prevent future attacks. Among other responsibilities, the Secretary is to coordinate the distribution of information between federal agencies and state and local governments. Furthermore, the act requires the new department's Under Secretary for Information Analysis and Infrastructure Protection to disseminate, as appropriate, information analyzed by the department to other federal, state, and local government agencies with homeland security roles; to consult with state and local governments to ensure appropriate exchanges of information (including law-enforcement-related information) relating to threats of terrorism; and to coordinate with elements of the intelligence community and with federal, state, and local law enforcement agencies, and the private sector, as appropriate. Additionally, a subtitle of the Homeland Security Act, titled the Homeland Security Information Sharing Act, requires the President of the United States to prescribe and implement governmentwide procedures for determining the extent of sharing, and for the actual sharing, of homeland security information between federal agencies and state and local personnel, and for the sharing of classified (and sensitive but unclassified) information with state and local personnel. To date, these procedures have not been promulgated, although the President has recently assigned this function to the Secretary of Homeland Security.¹³

Furthermore, several national strategies that have been developed include information sharing as major initiatives. Both the *National Strategy for Homeland Security* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* include, as objectives, improving information sharing between intelligence and law enforcement agencies at all levels of government. In addition, FBI increased the number of its Joint Terrorism Task Forces, from 35, as of September 11, 2001, to

¹³ Executive Order No. 13311, *Homeland Security Information Sharing*, July 29, 2003.

66, as of March 2003. Federal, state, and local law enforcement officials can interact to prevent terrorist attacks and share information in investigations of terrorist events through the task forces. State and city governments have also implemented several initiatives to improve the information-sharing process, both within their jurisdiction as well as with participants from other levels of government.

Information-Sharing Initiatives Are Not Well Coordinated

Congress passed legislation and the President issued strategic plans to improve the sharing of information to fight terrorism. The Department of Homeland Security was given the responsibility to coordinate the distribution of information between federal agencies, and state and local governments, and private industry. However, the department is in the early phases of determining how to execute this responsibility. In the meantime, some federal agencies and state and city governments undertook initiatives on their own to improve sharing. However, these actions are not well coordinated and consequently risk duplicating efforts. In addition, without coordination, these actions may not be mutually reinforcing and may create information-sharing partnerships that do not necessarily include all agencies needing access to the information.

Legislation and Strategies to Improve Information Sharing

After the September 11, 2001, attacks, Congress took legislative action to improve information sharing. Several national strategies, such as the *National Strategy for Homeland Security* contain actions to improve sharing as well.

The Homeland Security Act directs the President to prescribe and implement procedures for sharing homeland security information between federal agencies and with appropriate state and local government personnel (a function since assigned by the President to the Secretary of Homeland Security). The act also created the Department of Homeland Security, which consolidated 22 federal agencies with homeland security missions into a single department. Within the department, the Office of State and Local Government Coordination and the Office of Private Sector Liaison were created to provide state and local governments and appropriate private-sector representatives with regular information, research, and technical support to assist local efforts at securing the homeland. According to the department, these offices will give these participants one primary federal contact instead of many to meet their homeland security needs.

Since September 11, 2001, the administration has developed several strategies containing actions to improve information sharing and charge DHS, FBI, and other government components with responsibility to perform these actions. For example, the *National Strategy for Homeland Security* (July 2002), the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Feb. 2003), and the *National Strategy to Secure Cyberspace* (Feb. 2003) have, as one of their priorities, actions to promote information sharing between federal agencies and with state and city governments, law enforcement and intelligence agencies, and the private sector.¹⁴

The *National Strategy for Homeland Security* specifies that the federal government will “build a national environment that enables the sharing of essential homeland security information horizontally across each agency of the federal government and vertically among federal, state, and local governments, private industry, and citizens” by integrating all participants and streamlining the sharing process. The strategy contains initiatives to declassify documents to facilitate sharing, integrate databases at all levels of government, and provide for a secure method of sharing information. Similarly, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* has initiatives to facilitate information sharing by improving processes for domestic threat data collection, analysis, and dissemination to state and local governments as well as with private industry. This strategy calls on DHS to lead the effort to (1) define sharing requirements, (2) establish processes for providing and receiving information, and (3) develop technical systems to share sensitive information with public-private stakeholders. The *National Strategy to Secure Cyberspace* has initiatives to improve and enhance public-private information sharing involving cyber attacks by establishing, among other things, protocols for ensuring that information voluntarily provided by the private sector is securely stored and maintained.

The Department of Homeland Security has several initiatives to improve the sharing of information that could be used to protect the homeland. In particular, it is developing a homeland security enterprise architecture that, among other actions, will integrate sharing between federal agencies

¹⁴ See U.S. General Accounting Office, *Combating Terrorism: Observations on National Strategies Related to Terrorism*, [GAO-03-519T](#) (Washington, D.C.: Mar. 3, 2003) for a list of 10 strategies relating to terrorism. *The National Money Laundering Strategy* (July 2002) also calls for enhanced information sharing with the financial community to identify methods used by terrorist supporters to raise money.

and between the federal government, state and city governments, and the private sector. According to DHS, its enterprise architecture is a business-based framework for cross-agency improvement and will provide DHS with a new way of describing, analyzing, and integrating the data from the agencies, thus enabling DHS to “connect the dots” to better prevent terrorist attacks and protect people and infrastructure from terrorism. Architecture working groups were established to collect, organize, and publish the baseline information-sharing structure for the major components that were transitioned to DHS. According to DHS officials, this effort will be completed by June 2003. The working groups will also be used to integrate the state and city governments, and the private sector. By September of 2003, the department anticipates it will have a plan that provides a phased approach to achieving information sharing between the federal government, states, cities, and the private sector. The department anticipates beginning to implement the plan in November 2003.

Initiatives Risk Duplicating Efforts and May Limit Access for Some Entities

Other federal agencies, and state and city homeland security participants have implemented several initiatives to promote information sharing, yet these initiatives are not well coordinated and may inadvertently limit access to information to those entities that are not part of the initiatives. Nonetheless, the initiatives seek to fulfill a perceived information requirement not yet fully addressed by the federal intelligence community, and include both technological solutions as well as management and communication solutions. However, these initiatives may be duplicating DHS and other federal efforts already under way, and, in some cases, may create information-sharing partnerships that actually limit access to information to only those agencies that are party to the initiatives.

Sensing an urgency to improve their abilities to effectively perform their homeland security duties, other federal agencies, and state and city participants have implemented several initiatives to promote sharing with others from different levels of government.¹⁵ However, it is unclear how these initiatives, while enhancing individual organization sharing, will contribute to national information-sharing efforts. The Departments of Defense and Justice have established initiatives using technology to better gather, analyze, and share information with other homeland security

¹⁵ We did not attempt to build a comprehensive list of all sharing initiatives. In our discussions with officials from all levels of government and from our survey, we were able to identify some initiatives that were ongoing.

participants. These initiatives include expanding existing mechanisms for sharing; participating in information-sharing centers like FBI's Joint Terrorism Task Forces; establishing new information-sharing centers; and working with federal, state, and city agencies to integrate databases. Also, the new Terrorist Threat Integration Center, which began operations May 1, 2003, was created to fuse, analyze, and share terrorist-related information collected domestically and abroad. It is an interagency joint venture that reports directly to the Director of Central Intelligence in his capacity as statutory head of the intelligence community. The center will be comprised of elements of DHS, FBI's Counterterrorism Division, the Director of Central Intelligence Counterterrorist Center, the Department of Defense, and other participating agencies. According to the President, the center is to "close the seam" between the analysis of foreign and domestic intelligence and will have access to all sources of information.

In responding to our survey, 85 percent (or 34 of 40) of the responding states and 70 percent (or 160 of 228) of the responding cities said they were currently participating in information-sharing centers, including FBI's Joint Terrorism Task Forces. Nonetheless, according to the survey results, many participants expressed a need for still more interaction with other homeland security participants to coordinate planning, develop contacts, and share information and best practices.

In addition to the federal government, several states and cities have implemented their own initiatives to improve sharing. For example, the state of California has established a clearinghouse for all terrorist-related activities and investigations. The clearinghouse collects, analyzes, and disseminates information to its law enforcement officers, other law enforcement agencies, and FBI. The City of New York established a counterterrorism committee comprising FBI, the New York State Office of Public Security, and the New York City Police Department to share information and promote joint training exercises. Officials from the Central Intelligence Agency acknowledged that states' and cities' efforts to create their own centers are resulting in duplication and that some cities may be reaching out to foreign intelligence sources independently from the federal government. These officials emphasized that state and local authorities should work through the Joint Terrorism Task Forces to receive the information they require. Appendix II contains examples of other initiatives that various information-sharing participants have expanded and/or implemented to protect the homeland since September 11, 2001.

In written comments to our survey, some respondents indicated that avoiding duplication and redundancy were some of the reasons they were not joining or establishing new information-sharing centers. For example, rather than establishing local or regional databases—as some states and cities have done—some respondents recommended creating a national terrorism intelligence and information network and computer database. However, in order to build a comprehensive national plan that integrates multiple sharing initiatives (including those that integrate databases), the federal government must first be aware of these efforts. In a speech to the National Emergency Managers Association in February 2003, the Secretary of Homeland Security asked states to inform his department of newly created initiatives when they learn of them. However, it is not clear if states and cities have provided DHS with this information and whether DHS has taken actions on the basis of the information.¹⁶ As a result, federal efforts to integrate initiatives may overlook some state or city initiatives that could help to improve information sharing and enhance homeland security.

Another way that information-sharing initiatives may limit access to information for some entities is through partnerships that promote information sharing between the partners but exclude those not participating. Some federal agencies may try to meet their information needs by forming partnerships with other agencies outside the purview of DHS and its ongoing national strategy efforts. Thus, these organizations may concentrate on local threat information and unknowingly have vital information that, when combined with national or regional information, could indicate an impending attack or help prepare for an attack.

Current Information-Sharing Process Not Perceived As Effective

In spite of legislation, strategies, and initiatives to improve information sharing, federal agencies and state and city governments generally do not consider the current information- and intelligence-sharing process to be effective. The documents that we reviewed, and officials from federal agencies, states, and cities we interviewed, indicated that they did not perceive the sharing process as working effectively. And, in our survey, fewer than 60 percent of federal, state, and city respondents rated the current sharing process as “effective” or “very effective.” Respondents

¹⁶ In July 2002, the Office of Homeland Security published a document, *State and Local Actions for Homeland Security*, in which the office asked states, cities, and county governments to list initiatives for homeland security. However, we were unable to meet with the Office of Homeland Security to determine how this information will be used.

identified three systemic problems. First, they believe that needed information is not routinely provided. Second, the information that they do receive is not always timely, accurate, or relevant. Third, they feel that the federal government still perceives the fight against terrorism to be generally a federal responsibility and consequently does not integrate state and city governments into the information-sharing process. An information-sharing process characterized by such systemic problems or shortcomings could contribute to a failure to detect a pending attack or prepare for an attack.

Further Improvement Is Needed in the Information-Sharing Process

According to recent reports and testimony, further improvement is needed in the information-sharing process to better protect the homeland. Federal officials have stated that information-sharing problems still exist. We have also expressed concerns about information sharing in previous reports and testimonies, as shown in the following examples:

- Inquiries into the events of September 11, 2001, have highlighted ongoing problems with the existing sharing process and the need for improvement. Both the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have, in a joint inquiry in 2002, stated that much information exists in the files and databases of many federal, state, and local agencies.¹⁷ However, that information is not always shared or made available in timely and effective ways to decision makers as well as analysts to better accomplish their individual missions.
- In October 2002, the Staff Director of the Joint Inquiry Staff that investigated the September 11, 2001, intelligence issues testified that information sharing was inconsistent and haphazard.
- On December 15, 2002, the Gilmore Commission¹⁸ concluded that information sharing had only marginally improved since the September 11, 2001, attacks, and that despite organizational reforms, more attention, and better oversight, the ability to gather, analyze, and disseminate critical information effectively remained problematic. Additionally, the commission reported that current information-sharing practices neither

¹⁷ Testimony given by Eleanor Hill, Director of Joint Inquiry, before the Joint Intelligence Committee, U.S. Congress, from September 18, 2002, and October 17, 2002.

¹⁸ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Fourth Annual Report IV, Implementing the National Strategy* (Arlington, Va.: Dec. 15, 2002). The Advisory Panel, chaired by former Virginia Governor James Gilmore, was established by section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105-261.

transfer to local authorities the information they need, nor adequately assesses the information collected by local authorities.

We have also expressed concerns about homeland security in previous reports and testimonies that documented the lack of standard protocols for sharing information and intelligence; the lack of partnerships between the federal, state, and local governments; and the lack of a unified national effort to improve the sharing process. In those reports, we concluded that more effort is needed to integrate the state and local governments into the national sharing process.¹⁹ In our report on the integration of watch list databases that contain information on known terrorists, we found that sharing is more likely to occur between federal agencies than between federal agencies and state or local government agencies because of overlapping sets of data and different policies and procedures.²⁰

Participants Do Not Perceive Current Information-Sharing Process as “Effective” or “Very Effective”

Our work involving the interviewing of cognizant officials, reviewing information-sharing documents, and analyzing the results of our survey indicated that information-sharing participants do not perceive the current process as “effective” or “very effective.” Without an effective sharing process, it is not clear how important information obtained by federal, state, or city agencies could be connected to relevant information held by other agencies and potentially pointing to an imminent attack.

In a position paper, the Major Cities Chiefs Association stated that the federal government needed to better integrate the thousands of local police officers into the sharing process and by not doing so, the federal government is not taking advantage of their capabilities.²¹ In March 2002, the National Governors Association stated that law enforcement and public safety officers do not have access to complete, accurate, and timely

¹⁹ U.S. General Accounting Office, *Homeland Security: Key Elements to Unify Efforts Are Underway but Uncertainty Remains*, GAO-02-610 (Washington, D.C.: June 7, 2002) and *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).

²⁰ U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322 (Washington, D.C.: Apr. 15, 2003). This is an example of a lack of effective integration.

²¹ Major Cities Chiefs Association, *Terrorism, the Impact on State and Local Law Enforcement*, Intelligence Commanders Conference Report (June 2002). (<http://www.neiassociates.org/mccintelligencereport.pdf>)

information. As a result, critical information is not always shared at key decision points, sometimes with tragic consequences.²² The International Association of Chiefs of Police testified in June 2002 that the current sharing process is not effective because state and city governments are not fully integrated into a national sharing process.²³

We conducted our survey nearly a year later and found little change. Our survey results indicate that participants do not perceive the current sharing of information to fight terrorism to be “effective” or “very effective,” regardless of the level of government with whom they shared information. In our survey we asked all respondents to indicate the extent of effectiveness when they shared information with the other government levels. For example, we asked the federal respondents to rate their responses from “not effective” to “very effective” when they shared information with other state and city governments. Table 2 shows the different perceived levels of effectiveness within the three levels of government.

Table 2: Percentage of Federal, State, and City Respondents That View Their Sharing Relationships with One Another As Effective or Very Effective

Jurisdiction	Percent			
	Federal sharing with	State sharing with	Large-city sharing with	Small-city sharing with
Federal	44	35	37	29
State/Intrastate	13	43	51	42
City/Intracity	13	40	57	54

Source: GAO.

Notes: Although our results represent a substantial number of governmental entities, the results do not represent the entire population of governmental entities involved in information sharing.

Number of federal agency respondents = 16; number of state respondents = 40; number of large-city respondents = 106; and number of small-city respondents = 122.

As shown in table 2, generally fewer than 60 percent of the respondents felt that the information-sharing process was “effective” or “very effective.”

²² National Governors’ Center for Best Practices, *Improving Public Safety Through Justice Information Sharing* (Washington, D.C.: March 2002).

²³ Statement of the President of the International Association of Chiefs of Police before the Committee on Governmental Affairs, U.S. Senate, June 26, 2002.

In particular, only 13 percent of the federal agencies that completed our survey reported that when sharing information with the states and cities, the current process was “effective” or “very effective.” One reason for this low percentage may be due to the historic reluctance of the federal government to share terrorism information with states and cities. On the other hand, 51 percent of large-city respondents reported that their sharing relationships with states was “effective” or “very effective,” reflecting a closer historic relationship that cities have with their states.

Systemic Problems Account for Perception That Process Is Ineffective

Federal, state, and city authorities do not perceive the current sharing process as “effective” or “very effective” because they believe (1) that they are not routinely receiving the information they believe they need to protect the homeland; (2) that when information is received, it is not very useful, timely, accurate, or relevant; and (3) that the federal government still perceives the fight against terrorism to be generally a federal responsibility. Consequently, comprehensive policies and procedures to effectively integrate state and city governments into the process of determining requirements, analyzing and disseminating information, and providing feedback have not been established. As a result, opportunities may be routinely missed to engage state and city officials in obtaining information from the federal government and providing the federal government with information that could be important in the war against terrorism.

Participants Are Not Routinely Receiving Needed Information

The federal, state, and city officials that completed our survey indicated that certain information was perceived to be extremely important to execute their homeland security duties, but they reported that they were not routinely receiving it.²⁴ In the survey, we listed different types of homeland-security-related information and asked all respondents to indicate the extent to which they needed and received the information. With few exceptions, the federal, state, and city agencies that completed our survey indicated that they are typically receiving less than 50 percent

²⁴ For the purpose of this report, we consider information as extremely important to providing homeland security if respondents reported that they “needed” or “critically needed” the types of information that we listed in our survey. We did not determine if these needs were valid.

of the categories of information they seek.²⁵ While our survey results found that state and local agencies were generally dissatisfied with the results of information sharing with the federal government, federal agencies were just as dissatisfied with the flow of information from state and city agencies.

As shown in table 3, the majority of the states and cities reported that they needed many of the types of information listed in our survey question. For example, 90 to 98 percent of the states and large and small cities that completed our survey reported that they needed specific and actionable threat information; yet only 21 to 33 percent of them reported that they received this information. However, more than 50 percent of all respondents reported that they were receiving needed broad threat information.

Table 3: Perceptions of Information Needed and Regularly Received

Category	Percent							
	Federal agencies (n = 16)		States (n = 40)		Large cities (n = 106)		Small cities (n = 122)	
	Needed	Received	Needed	Received	Needed	Received	Needed	Received
Broad threat information	75	75	93	75	81	77	72	57
Specific and actionable threat information	88	56	98	33	98	28	90	21
Movement of WMD by “friendly” authorities	56	19	83	23	77	6	66	6
Movement of WMD by terrorists	88	25	95	15	98	5	89	2
Movement of known terrorists	69	31	98	15	98	15	93	3
Activities of known terrorist support groups	69	25	93	18	97	15	90	2
Notification of ongoing federal investigations	88	25	90	23	90	23	87	7
Notification of federal arrests	81	25	90	33	92	23	89	7

²⁵ Areas where respondents indicated that they were receiving more than 50 percent of the information they seek included broad threat information (ranging from 57 to 75 percent), and, for the federal government respondents only, analysis of information within a national and international perspective (63 and 56 percent, respectively), and access to classified national security information (75 percent).

Category	Percent							
	Federal agencies (n = 16)		States (n = 40)		Large cities (n = 106)		Small cities (n = 122)	
	Needed	Received	Needed	Received	Needed	Received	Needed	Received
Notification of ongoing state investigations	75	13			92	17	87	4
Notification of state arrests	75	13			94	16	89	4
Notification of ongoing local investigations	63	13	93	33				
Notification of local arrests	63	13	88	33				
Access to classified national security information	88	75	80	28	60	13	43	6
Access to declassified national security information	75	56	85	45	75	33	60	15
Analysis of information within a regional perspective	81	50	95	25	97	24	88	7
Analysis of information within a national perspective	94	63	90	23	87	21	77	8
Analysis of information within an international perspective	88	56	83	28	69	17	64	4

Source: GAO.

Notes: Although our results represent a substantial number of governmental entities, the results do not represent the entire population of governmental entities involved in information sharing.

n = number.

WMD = weapons of mass destruction.

One reason that states and cities may not receive needed threat information is that the information may not be available. For example, actionable threat information is rarely available according to federal intelligence officials we interviewed; however, if available, these officials told us that they would not hesitate to provide those who needed it with the information. Nonetheless, if the information is classified, Executive Order no. 12968 specifies that the information is not to be shared unless the would-be recipients have the proper security clearances and a need-to-know. Thus, the issue arises of how actionable threat information

can be shared with state and local personnel without unauthorized disclosure of classified information by federal officials.²⁶ Longstanding agency practices may also account for poor information sharing and may include the institutional reluctance of federal officials to routinely share information with local law enforcement officials.

Without the information that they feel they need, states and cities, as well as the federal government, may not be adequately prepared to deter future attacks. Consequently, the nation's ability to effectively manage the risk of future attacks may be undermined. For example, the National Governors Association, the National League of Cities, and the National Emergency Management Association have all stated that they need timely, critical, and relevant classified and nonclassified information about terrorist threats so that they can adequately prepare for terrorist attacks. And the Major Cities Chiefs Association stated that law enforcement officers need background information on terrorism, the methods and techniques of terrorists, and the likelihood of an imminent attack. With this information, the association believes that law enforcement would have the background from which it could take seemingly random or unconnected events—such as minor traffic violations—and place them into a larger context, thereby being able to perceive a bigger picture of potential attack or recognize the need to pass the information to an appropriate homeland security partner agency.

Information Received Not Very Timely, Accurate, or Relevant

Our survey results confirm the perception that the information that respondents do receive is not often seen as timely, accurate, or relevant. And, of the three aspects, respondents reported that timeliness was more of a problem than accuracy or relevancy. This supports a common complaint we heard from police chiefs—that they wanted timely information but would often receive information from national news sources at the same time that the public received it. This lack of timeliness was often attributed to the federal government's historic reluctance to share this type of information with local law enforcement officials. In the survey, we asked all respondents to indicate the extent to which the information they received from each other was timely, accurate, and relevant. Generally no level of government, including the federal

²⁶ The Homeland Security Act requires the President to address the sharing of classified information with state and local personnel in establishing procedures for facilitating homeland security information sharing.

government, was satisfied with the information received from the federal government, as shown in table 4.

Table 4: Survey Respondents Who Said the Information from the Federal Government Was Timely, Accurate, or Relevant

Federal sharing with	Timely		Accurate		Relevant ^a	
	Number	Percent	Number	Percent	Number	Percent
Federal (n = 16)	6	38	5	31	7	44
State (n = 40)	15	38	19	48	20	50
Large cities (n = 106)	24	23	41	39	42	40
Small cities (n = 122)	17	14	26	21	27	22

Source: GAO.

Notes: Although our results represent a substantial number of governmental entities, the results do not represent the entire population of governmental entities involved in information sharing.

n = number.

^aGreat to very great extent.

In particular, table 4 highlights these problems for large cities. Only 23 percent of the large cities reported that the information they received from the federal government was timely, and only 39 percent reported that it was accurate. Only 40 percent reported that the information received was relevant.

When state agencies were the source of information, federal and city agencies were also dissatisfied, as shown in table 5.

Table 5: Survey Respondents Who Said That Information from State Agencies Was Timely, Accurate, or Relevant

State sharing with	Timely		Accurate		Relevant ^a	
	Number	Percent	Number	Percent	Number	Percent
Federal (n = 16)	2	13	1	6	1	6
Large cities (n = 106)	32	30	36	34	31	29
Small cities (n = 122)	21	17	36	30	36	30

Source: GAO.

Notes: Although our results represent a substantial number of governmental entities, the results do not represent the entire population of governmental entities involved in information sharing.

n = number.

^aGreat to very great extent.

Table 5 shows that in general, large and small cities view the information they receive from their state as more timely, accurate, and relevant than when compared with the view of federal agencies when they receive information from the states. Few of the federal agencies that responded view state information received as timely, accurate, or relevant.

Similarly, few federal or state agencies that responded to our survey viewed information received from the cities as timely, accurate, or relevant, as shown in table 6.

Fighting Terrorism Still Seen as Generally a Federal Responsibility

Table 6: Survey Respondents Who Said That Information from City Agencies Was Timely, Accurate, or Relevant

Cities sharing with	Timely		Accurate		Relevant ^a	
	Number	Percent	Number	Percent	Number	Percent
Federal (n = 16)	2	13	2	13	1	6
State (n = 40)	14	35	17	43	10	25

Source: GAO.

Notes: Although our results represent a substantial number of governmental entities, the results do not represent the entire population of governmental entities involved in information sharing.

n = number.

^aGreat to very great extent.

Table 6 also shows that states view the information they receive from cities more favorably than the federal agencies that responded to our survey.

The nation’s fight against terrorism is still generally perceived to be a federal responsibility, at least in terms of preventing (in contrast to responding to) a terrorist attack. Even though states and cities develop important information on potential terrorist threats to the homeland, the federal government still has not established comprehensive policies or procedures to effectively integrate state and city governments into the process of determining requirements; gathering, analyzing, and disseminating information; and providing feedback. Nor has the federal government routinely recognized states and cities as customers in the information-sharing process.

Our survey results support the view that preventing terrorism is still perceived generally as a federal responsibility. We asked respondents to indicate the extent to which the elements of a sharing framework for receiving information from the federal government—such as clear guidance and access to needed databases—were in place at the various

governmental levels.²⁷ The existence of these elements would indicate to some extent the level that state and city governments were integrated into the sharing process. Specifically, we found that more elements of a sharing framework, such as clear guidance for providing and receiving information, are in place at the federal level than at the state or city level, indicating that terrorism-related information is managed more at the federal level.²⁸ Moreover, the lack of such elements at the state and city level nearly 2 years after the September 11, 2001, attacks may perpetuate the perception that the fight against terrorism remains generally a federal responsibility. State and city governments that completed our survey also indicated that they do not participate in national policy making regarding information sharing, which also helps maintain the perception. For example, 77 percent of the responding states, 92 percent of large cities, and 93 percent of small cities reported that they did not participate in this policy-making process. By involving states and cities, this process would help ensure a more unified and consolidated effort to protect the homeland, and provide opportunities to improve information sharing at the state and city levels.

The view that preventing terrorism is generally a federal responsibility is also reflected in the perception of the existence of barriers to providing information upwards or downwards. For example, according to the December 2002 report of the Gilmore Commission, the prevailing view continues to be that the federal government likes to receive information but is reluctant to share information with other homeland security partners. Furthermore, the commission stated that the federal government must do a better job of designating “trusted agents” at the state and local levels and in the private sector, and move forward with clearing those trusted agents.²⁹ In our survey, we listed a number of barriers and asked all

²⁷ In our survey, we listed over 20 elements of a sharing framework we believe would need to be in place at the various levels of government and would indicate that the states and cities were integrated into the sharing process. Some of these elements are “receiving feedback,” “having resources to analyze information,” and “routinely sharing information with others.” See app. IV for the survey results for this question.

²⁸ On March 4, 2003, the Director of Central Intelligence, the Attorney General, and the Secretary of Homeland Security signed an information-sharing memorandum. It is intended to mandate requirements and procedures for information sharing, use, and handling of analytic judgments among the federal intelligence community.

²⁹ Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, Dec. 15, 2002. Trusted agents would be state, local, and private-sector officials that would be given national security clearances in order to have better access to information.

respondents to indicate the extent to which these barriers hindered sharing with each other. Table 7 identifies the barriers that federal, state, and city agencies that responded to our survey believe exist in the current information-sharing process.

Table 7: Perceived Barriers Preventing Federal Agencies from Providing Other Federal Agencies, States, and Cities with Information

Category	Percent		
	Federal to federal	Federal to state	Federal to cities
Legal barriers	13	13	25
Authorities lack interest in information to be provided	6	0	0
Culture of “information superiority”	6	0	0
Concerns about jeopardizing ongoing investigations	13	13	0
Lack of confidence in ability to limit disclosure of information	6	19	6
Lack of confidence in ability to manage investigations	6	0	0
Concerns of disclosing sources and methods	6	25	19
Lack of integrated databases	38	38	31
Lack of clearances	NA	44	38
Difficulty with provision to secure, maintain, and destroy information	NA	44	50

Source: GAO.

Notes: Percentages include those respondents that answered “great-to-very great” on this question.

Although our results represent a substantial number of governmental entities, the results do not represent the entire population of governmental entities involved in information sharing.

NA = not applicable.

As shown in table 7, federal officials cited several barriers that they perceive prevent them from sharing information, including concerns over state and local officials’ ability to secure, maintain, and destroy classified information; their lack of security clearances; and the absence of integrated databases. However, these perceived barriers were seen to exist by only a few respondents and could be overcome. For example, state and local police routinely handle and protect law-enforcement-sensitive information to support ongoing criminal investigations, which suggests that—with proper training and equipment—officials of these governments could handle other types of sensitive information as well.

As mentioned earlier, the Homeland Security Act requires the President, in establishing information-sharing procedures, to address the sharing of classified and sensitive information with state and local personnel. Congress suggested in the Homeland Security Act that the procedures could include the means for granting security clearances to certain state and local personnel, entering into nondisclosure agreements (for sensitive but unclassified information), and the increased use of information-sharing partnerships that include state and local personnel. For example, Congress found that granting security clearances to certain state and local personnel is one way to facilitate the sharing of information regarding specific terrorist threats between federal, state, and local levels of government.³⁰ We found that the federal government has issued security clearances to state or local officials in limited circumstances and is increasing the number of such clearances. The Federal Emergency Management Agency has provided certain state emergency management personnel with security clearances for emergency response purposes, but other federal agencies, including FBI, have not recognized the validity of these security clearances. For FBI, this lack of recognition could prevent it from providing state emergency management personnel with information. At the same time, FBI has undertaken some initiatives to provide certain state officials with clearances and could clearly expand this program at the state and city levels, if officials believe that doing so will address a perceived impediment to information sharing. And DHS is also developing a new homeland security level classification for information to improve sharing.

For their part, states and cities reported few barriers in their ability to provide the federal government with information, while federal agencies cited a number of barriers to sharing. As shown in table 7, state and city agencies perceived that the federal government faces few barriers in sharing information. Appendix V details the barriers that states and cities perceive to providing federal authorities with information.

All categories of survey respondents identified the lack of integrated information systems as the single most common barrier to information sharing across all levels of government. The Markle Foundation stated in its report that federal agencies have seen the information and homeland

³⁰ Congress also found that methods exist to declassify, redact, or otherwise adapt classified information so that it may be shared with state and local personnel without the need for granting additional security clearances.

security problem as one of acquiring new technology.³¹ For example, for fiscal year 2003, FBI budgeted \$300 million for new technology, the Transportation Security Administration has budgeted \$1 billion over several years, and the former Immigration and Naturalization Service (whose function is now within DHS) has a 5-year plan for \$550 million. However, the foundation reports that almost none of this money is being spent to solve the problem of how to share this information between federal agencies and with the states and cities. The foundations' report states that when it comes to homeland security and using integrated information systems, adequate efforts and investments are not yet in sight. And in recent testimony, we stated that DHS must integrate the many existing systems and processes within government entities and between them and the private sector required to support its mission.³²

Conclusions

With the current decentralized information-sharing process in which actions to improve sharing are not organized, and participants at all levels of government and the private sector are not well integrated into the scheme, the nation may be hampered in its ability to detect potential terrorist attacks and effectively secure the homeland. Additionally, the lack of coordination of the various information-sharing initiatives continues to hamper the overall national effort to effectively share information that could be used to prevent an attack.

DHS has initiated an enterprise architecture to provide a road map to address information-sharing issues with all levels of government and the private sector. It is important that this be done in such a way as to effectively integrate all levels of government and the private sector into an information-sharing process. Until then, it is not clear how the department will coordinate the various information-sharing initiatives to eliminate possible confusion and duplication of effort. Participants risk duplicating each other's efforts and creating partnerships that limit access to information by other participants, thus increasing the risk that decision makers do not receive useful information; developing initiatives that are

³¹ See Markle Foundation, *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force*, (Washington, D.C.: Oct. 2002).

³² See U.S. General Accounting Office, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, [GAO-03-715T](#) (Washington, D.C.: May 8, 2003).

not mutually reinforcing; and potentially unnecessarily increasing the cost of providing homeland security.

The failure to fully integrate state and city governments into the information-sharing policy-making process deprives the federal government of the opportunity to (1) obtain a complete picture of the threat environment and (2) exploit state and city governments' information expertise for their own areas, with which they are uniquely familiar.

Finally, the effectiveness of the information-sharing process to provide timely, accurate, and relevant information is also in question, creating a risk that urgent information will not get to the recipient best positioned to act on it in a timely manner. Until the perceived barriers to federal information sharing are addressed, the federal government may unnecessarily, and perhaps inadvertently, be hampering the state and city governments from carrying out their own homeland security responsibilities.

States, cities, and the private sector look to the federal government—in particular the Department of Homeland Security—for guidance and support regarding information-sharing issues. If DHS does not effectively strengthen efforts to improve the information-sharing process, the nation's ability to detect or prepare for attacks may be undermined.

Recommendations for Executive Action

We recommend that, in developing its enterprise architecture, the Secretary of Homeland Security work with the Attorney General of the United States; the Secretary of Defense; the Director, Office of

Management and Budget; the Director, Central Intelligence; and other appropriate federal, state, and city authorities and the private sector to ensure that the enterprise architecture efforts

- incorporate the existing information-sharing guidance that is contained in the various national strategies and the information-sharing procedures required by the Homeland Security Act to be established by the President;
- establish a clearinghouse to coordinate the various information-sharing initiatives to eliminate possible confusion and duplication of effort;
- fully integrate states and cities in the national policy-making process for information sharing and take steps to provide greater assurance that actions at all levels of government are mutually reinforcing;

-
- identify and address the perceived barriers to federal information sharing; and
 - include the use of survey methods or related data collection approaches to determine, over time, the needs of private and public organizations for information related to homeland security and to measure progress in improving information sharing at all levels of government.

As you know, 31 U.S.C. 720 requires the head of a federal agency to submit a written statement of the actions taken on our recommendations to the Senate Committee on Governmental Affairs and the House Committee on Government Reform not later than 60 days after the date of this report. A written statement must also be sent to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report.

Agency Comments and Our Evaluation

We presented a draft of this report to the Departments of Homeland Security, Defense, and Justice; and to the Director of Central Intelligence. The Departments of Homeland Security, Defense, and Justice provided written comments. The Central Intelligence Agency provided technical comments. All the departments, except the Department of Justice, concurred with our report.

The Department of Homeland Security concurred with our report and recommendations. The department added that it has made significant strides to improve information sharing. For example, the department pointed out that it is in the process of providing secure telephones to the governors and security clearances to the Homeland Security Advisors in every state so that relevant classified information can be shared. The department also pointed out that further progress will require a thoughtful, prudent, and deliberate approach. However, it cautioned that issuing the first draft of the national homeland security enterprise architecture could go beyond the September 2003 target because of the time it may take to obtain appropriate interagency coordination. The department's comments are reprinted in their entirety in appendix VI.

DOD concurred with our recommendations. DOD's comments are reprinted in their entirety in appendix VII.

The Central Intelligence Agency provided technical comments that we incorporated into our draft as appropriate.

On the other hand, the Department of Justice did not concur with our report and raised several concerns. The department stated that our draft report reaches sweeping and extraordinarily negative conclusions about the adequacy of the governmental sharing of information to prevent terrorism and that (1) our conclusions are fundamentally incorrect and unsupported by reliable evidence; (2) our review was beyond our purview; and (3) an evaluation of information sharing requires a review of intelligence sharing which by long standing practice the executive branch provides to Congress but not us, thus we may not be able to provide useful information to Congress. We disagree.

First, we used reliable evidence from a variety of sources, including the Central Intelligence Agency; the Anser Institute of Homeland Security; the Joint Inquiry into the Terrorist Attacks of September 11, 2001; reports of the RAND Institute and the Markle Task Force on National Security in the Information Age; testimony before congressional committees by federal, state, and local officials; interviews that we conducted with federal, state, and local agency officials and associations representing the International Association of Chiefs of Police, the U.S. Conference of Mayors, the National League of Cities, and the National Sheriffs Association; and our survey results. Moreover, over 100 cities with populations in excess of 100,000, over 120 cities with populations of under 100,000, and 40 states responded to our survey, representing a substantial number of governmental entities providing us with evidence of information-sharing shortcomings. These organizations are involved in information collection and analysis, have conducted well respected studies on information-sharing issues, or have significant experience in providing for homeland security through law enforcement or emergency management at the state and the local level, and are recognized as authorities in their fields of endeavor. Our conclusions are based on this body of evidence. Our complete scope and methodology is shown in appendix I.

Second, the Department of Justice stated that “our review of intelligence activities is an arena that is beyond GAO’s purview” and that providing GAO with information on intelligence sharing “would represent a departure from the long-standing practice of Congress and the executive branch regarding the oversight of intelligence activities.” The Department of Justice’s impression that our review was a review of intelligence activities is incorrect. As our report clearly indicates, the oversight of intelligence activities was not an objective or focus of our review, which did not require our access to intelligence information or involve our evaluation of the conduct of actual intelligence activities. Rather, our review considered the use of intelligence information in general in the

context of the broader information-sharing roles and responsibilities of various homeland security stakeholders (including the intelligence community). However, even if our review could be construed as involving intelligence activities, we disagree that such a review is outside GAO's purview. We have broad statutory authority to evaluate agency programs and activities and to investigate matters related to the receipt, disbursement, and use of public money. To carry out our audit responsibilities, we have a statutory right of access to agency records applicable to all federal agencies. Although our reviews in the intelligence area are subject to certain limited restrictions,³³ we regard such reviews as fundamentally within the scope of our authority.

Third, as to the department's assertion that providing GAO with information on intelligence sharing practices would represent "a departure from long-standing practice," we believe our review in this area furthers congressional oversight but does not require reviewing intelligence sharing practices. For example, we are not aware that the views of state and local government officials on information sharing contained in our report have previously been provided to Congress in a comprehensive manner, their views are not dependent on whether we do or do not have access to intelligence sharing practices, and the department did not indicate that this is the case in asserting that Congress is already receiving sufficient information from the executive branch. Moreover, we did not review the extent to which the executive branch provides useful information to Congress so we cannot comment on the department's assertion. Nonetheless, as our report clearly discusses, numerous state and local government officials believe that they had not received the information that they need from federal agencies. It would have also been useful, had the department shared with us its views on information sharing for homeland security. We believe Congress should have available such information in making informed decisions in this area. The department's comments are reprinted in appendix VIII.

³³ These include narrow legal limitations on our access to certain "unvouchered" accounts of the Central Intelligence Agency and on our authority to compel our access to foreign intelligence and counterintelligence information. For more detail, see our testimony, 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).

We are sending copies of this report to appropriate congressional committees. In addition, we are sending copies of the report to the Secretaries of Homeland Security, Defense, Commerce, Agriculture, Transportation, and the Treasury; the Attorney General; the Director of Central Intelligence; and the Director, Office of Management and Budget. We will make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions about matters discussed in this report, please contact me at (202) 512-6020 or by E-mail at deckerrj@gao.gov. GAO contacts and staff acknowledgements are listed in appendix IX.

Sincerely yours,

A handwritten signature in black ink that reads "Raymond J. Decker". The signature is written in a cursive, slightly slanted style with a long horizontal stroke at the end.

Raymond J. Decker, Director
Defense Capabilities and Management

Appendix I: Scope and Methodology

Our objectives were to determine (1) what initiatives have been undertaken to improve the sharing of information that could be used to protect the homeland and (2) whether federal, state, and city officials believe that the current information-sharing process is effective.

To achieve the first objective, we reviewed documents to determine legislative initiatives and other initiatives detailed in national strategies to include the *National Strategy for Homeland Security*, the *National Strategy for Combating Terrorism*, the *National Military Strategic Plan of the United States of America*, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, the *National Strategy to Secure Cyberspace*, and the *National Security Strategy of the United States of America*. We also reviewed federal, state, and city initiatives to share information. We interviewed officials from the Department of Justice, the Federal Bureau of Investigation (FBI), and the Defense Intelligence Agency on their initiatives to share information with state and city entities, and discussed information or intelligence-sharing policies and procedures with officials from the Central Intelligence Agency; the Department of Defense (DOD), Departments of Commerce, Agriculture, the Treasury, and Transportation; the U.S. Coast Guard; and DOD's new U.S. Northern Command. We also surveyed a select group of federal, state, and city organizations to obtain information on whether they were involved in information-sharing initiatives.

To determine whether the current information-sharing process is perceived as effective by federal, state, and city governments, we interviewed officials from DOD's Office of the Inspector General and the Defense Intelligence Agency; FBI and the Office of Intelligence Policy and Review within the Department of Justice; the U.S. Coast Guard; the Treasury Department and the U.S. Customs Service; the Department of Commerce; and the U.S. Department of Agriculture. We also interviewed representatives from the California Department of Justice, city and county of Los Angeles law enforcement authorities; the Director of Emergency Management for the District of Columbia; and the chiefs of police of Baltimore, Maryland; and Dallas, Fort Worth, and Arlington, Texas. We also interviewed representatives of professional organizations and research organizations, including the International Association of Chiefs of Police, the National Sheriffs Association, Police Executive Research Forum, the U.S. Conference of Mayors, the National League of Cities, the RAND Institute, the Center for Strategic and International Studies, and ANSER Institute for Homeland Security. To supplement our interviews, we reviewed studies and testimonies before Congress. Among the documents we reviewed are the testimonies of the President of the International

Chiefs of Police before the Senate Committee on Governmental Affairs, June 26, 2002; the former Central Intelligence Agency General Counsel before the aforementioned committee, February 14, 2003; and the Chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction before the aforementioned committee, February 14, 2003, and also the U.S. Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, October 1, 2002. We also reviewed the position papers of the RAND Institute, International Association of Chiefs of Police, Markle Task Force on National Security in the Information Age, and others.

Use of a Survey to Supplement Interviews and Review of Documents

To achieve both objectives, we conducted a survey to augment our interviews and review of testimonies, documents, and position papers. We surveyed all 29 federal intelligence and law enforcement agencies; 50 state homeland security offices; and 485 cities, including all cities with a population of 100,000 or greater, and 242 representing a random sample of cities with a population of between 50,000 and 100,000. The city surveys were directed to the mayors; however, the mayors frequently delegated the task of completing the survey to career employees such as chiefs of police, city managers, directors of emergency management offices, assistants to the mayors, and others. The survey was not sent to the private sector, although we recognize that it has a sizeable role in homeland security by virtue of owning about 80 percent of the critical infrastructure in the United States. The survey collected information on the types of information needed by participants, the extent that this information was received and provided, the sources and usefulness of the information, and the barriers that prevent participants from sharing. However, the survey did not attempt to validate the information needs of any level of government. To ensure the validity of the questions on the survey, we pretested it with officials from the Office of the Secretary of Defense, the Defense Intelligence Agency; the homeland security directors for the states of North Dakota and Florida; the police chiefs from the cities of Dallas, Fort Worth, and Arlington, Texas; and the Director of Emergency Management for the District of Columbia. We subsequently followed up the surveys with several phone calls and E-mail messages to all federal and state agencies surveyed, and a large number of cities to increase our response rate.

Of the 485 surveys sent to the cities, 228, or 47 percent, responded. The 257 cities that did not respond might have answered the survey differently from those that did; however, we could not determine this. Therefore, we present the results of those cities that did complete the surveys knowing

that the nonresponders could have answered differently. Where applicable in the report, we present the results of large and small cities separately, unless noted otherwise. Also, when presenting survey results, we judgmentally benchmarked the response level we believed would be acceptable for an information-sharing process that is so vital to homeland security. For example, for a process of this importance, we believe that respondents should perceive that the overall sharing process is “effective” or “very effective” and not “moderately effective” or lower.

The scope of this review did not include the federal government’s critical infrastructure protection efforts, for which we have made numerous recommendations over the last several years. We also did not include the private sector, although we recognize the importance of this sector in that it owns about 80 percent of the nation’s infrastructure. Critical infrastructure protection efforts are focused on improving the sharing of information on incidents, threats, and vulnerabilities, and the providing of warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments, and the private sector.

We conducted our review from June 2002 through May 2003 in accordance with generally accepted government auditing standards.

Appendix II: Selected Initiatives to Promote Information Sharing

In order to judge the extent of initiatives, judge efforts to share more information, and identify possible duplication of efforts, we gathered documents that outlined these efforts. Also, in our survey, respondents identified initiatives and efforts they were involved with. The following table is not exhaustive, since all respondents did not complete this survey question; however, it illustrates potential duplication of efforts between the federal, state, and city governments.

Table 8: Initiatives and Efforts to Share More Information

Name	Lead agency	Participants	Type and purpose
Terrorist Threat Integration Center	Under the direction of the Director of Central Intelligence	Elements of CIA, FBI, DHS, DOD, and other federal agencies	Began operation on May 1, 2003. The center will fuse and analyze terrorist-related information collected domestically and abroad to form a comprehensive threat picture. It is designed to be in one central location where information from all sources is shared, integrated, and analyzed. A senior U.S. government official, who will report to the Director of Central Intelligence, will head the center. As soon as an appropriate facility is available, FBI's Counterterrorism Division, the Director of Central Intelligence's Counterterrorism Center, and the center will relocate to a single new facility in order to improve collaboration and enhance the government's ability to prevent future attacks.
Joint Terrorism Task Force (JTTF)	FBI	Various local, state law enforcement entities, and other federal agencies	Increased from the pre-9/11 number of 33 to 66, the task forces are to enhance FBI's ability to promote coordinated terrorism investigations between its field offices and with its counterparts in federal, state, and local law enforcement agencies, and other federal agencies. FBI is providing task force agents and state and local law enforcement personnel with specialized counterterrorism training.
JTTF Information-Sharing Initiative	FBI	FBI, Illinois State Police, St. Louis Metropolitan Police Department, and other law enforcement entities	Piloted in St. Louis, this initiative integrates the investigative records of federal, state, and local agencies within a single database in order to provide area law enforcement with a single source for all criminal investigative records. This database provides investigators and analysts the ability to search the actual text of investigative records for names, addresses, phone numbers, scars, marks, and others. Each agency that enters data into the warehouse will be able to access it through four levels of security access.
JITF-CT/RISS.NET Information Exchange System (JRIES)	Joint Intelligence Task Force-Combating Terrorism (JITF-CT) of the Defense Intelligence Agency	DIA, California Anti-Terrorism Information Center (CATIC), NYPD	The Defense Intelligence Agency's newly created JITF-CT is working with the California Anti-Terrorism Information Center and the New York Police Dept.'s Counter Terrorism Division to build a system that connects the two entities in order to share information and intelligence about suspected terrorists' activities, cases, and arrests. One of JRIES' objectives is to provide information sharing functionality between agencies, which cross federal, state, and local boundaries.

**Appendix II: Selected Initiatives to Promote
Information Sharing**

Name	Lead agency	Participants	Type and purpose
Statewide Anti-Terrorism Unified Response Network (SATURN)	Massachusetts Executive Office of Public Safety	Massachusetts; Massachusetts state and local agencies; federal	SATURN was developed as a collaborative effort to provide a unified, effective response to terrorism by bringing together the public, fire, emergency management, and police officials from communities across Massachusetts along with key community leaders, state agencies, and the federal government to educate, prepare for, respond to, and prevent acts of terrorism. The SATURN network fosters the necessary communication, information sharing, training, and planning to enable the Commonwealth to prevent, prepare for, and respond to acts of terrorism.
Regional Domestic Security Task Force (RDSTF)	Florida (Florida Department of Law Enforcement)	Various Florida state agencies	The Florida Department of Law Enforcement established an RDSTF in each of the seven operational regions. Composed of subcommittees including Health/Medical, Emergency Medical Management, Law Enforcement, Fire Services, and Public Affairs, the RDSTFs work to improve Florida's ability to detect and prevent potential terrorist threats by collecting and disseminating intelligence and investigative information; facilitating and promoting ongoing security audits and vulnerability assessments; and protecting critical infrastructures.
CATIC	California Department of Justice	Federal, state, and local law enforcement	CATIC is the state's clearinghouse for all terrorist-related activities and investigations. CATIC collects, analyzes, and disseminates information to its 100,000 law enforcement officers, other law enforcement agencies, and FBI. Officials from the Defense Intelligence Agency are working to connect the CATIC system with the New York Police Department's Division of Counter-Terrorism.
Los Angeles County Sheriff's Department: Office of Homeland Security	Los Angeles County Sheriff's Department	Local law enforcement, state, county and federal agencies	The Los Angeles County Sheriff's Department established the Office of Homeland Security to enhance the department's response to potential threats related to local homeland security. The Office liaisons with federal, state, county, and local agencies with missions concerning the prevention and investigation of terrorist acts. In addition, the department created the Terrorism Early Warning Group in 1996 as an interdisciplinary group in which local, state, and federal agencies work together to share information, combine resources, and enhance the county's ability to identify and respond to acts and threats of terrorism.
New York Metropolitan Counter-Terrorism Committee	New York City law enforcement agencies	Various local, state, and federal law enforcement agencies	The committee comprises FBI, the New York State Office of Public Security, and the New York Police Department. The purpose of this committee is to share intelligence, share information regarding investigations, communicate information amongst its members, and promote joint training exercises. It has five subcommittees, including Intelligence and Investigations, which is working toward creating a repository of all interactions with suspicious individuals by metropolitan law enforcement agencies.
Maritime Domain Awareness (MDA)	U.S. Coast Guard		MDA is a concept that captures total awareness of vulnerabilities, threats, and targets of interest on the water. MDA is the comprehensive information, intelligence, and knowledge of all entities within America's waterways that could affect our safety, security, economy, or environment. According to the U.S. Coast Guard, MDA will constitute a significant force multiplier as missions expand against a background of limited resources.

Source: GAO.

Appendix III: Survey Responses Showing Categories of Homeland Security Information Deemed Needed by the Respondents

In order to establish a baseline for the information requirements of federal agencies, and state and city government officials, we provided survey respondents with a list of potential types of homeland security information and asked them to indicate what they thought they needed to meet their homeland security objectives. We then asked the respondents to tell us how frequently they received the information they perceived they needed. Table 9 is a summary of the types of information the respondents reported they needed or critically needed and the percentage that they frequently or regularly received the information. For example, 98 percent of state officials reported that they needed or critically needed specific and actionable threat information, while they also reported regularly receiving this type of information only 33 percent of the time.

Table 9: Needed to Critically-Needed Information and Intelligence and Frequently to Regularly-Received Information and Intelligence

Category	Percent							
	Federal agencies		States		Large cities		Small cities	
	Needed	Received	Needed	Received	Needed	Received	Needed	Received
Broad threat information	75	75	93	75	81	77	72	57
Specific and actionable threat information	88	56	98	33	98	28	90	21
Movement of WMD by “friendly” authorities	56	19	83	23	77	6	66	6
Movement of WMD by terrorists	88	25	95	15	98	5	89	2
Movement of known terrorists	69	31	98	15	98	15	93	3
Activities of known terrorist support groups	69	25	93	18	97	15	90	2
Notification of ongoing federal investigations	88	25	90	23	90	23	87	7
Notification of federal arrests	81	25	90	33	92	23	89	7
Notification of ongoing state investigations	75	13			92	17	87	4
Notification of state arrests	75	13			94	16	89	4
Notification of ongoing local investigations	63	13	93	33				
Notification of local arrests	63	13	88	33				
Access to classified national security information	88	75	80	28	60	13	43	6
Access to declassified national security information	75	56	85	45	75	33	60	15
Analysis of information within a regional perspective	81	50	95	25	97	24	88	7

**Appendix III: Survey Responses Showing
Categories of Homeland Security Information
Deemed Needed by the Respondents**

Category	Percent							
	Federal agencies		States		Large cities		Small cities	
	Needed	Received	Needed	Received	Needed	Received	Needed	Received
Analysis of information within a national perspective	94	63	90	23	87	21	77	8
Analysis of information within an international perspective	88	56	83	28	69	17	64	4

Source: GAO.

Note: Number of federal agency respondents = 16; number of state respondents = 40; number of large-city respondents = 106; and number of small-city respondents = 122.

Appendix IV: Survey Responses to Our Questions on the Elements of an Information-Sharing Process That Are Already in Place

GAO provided a list of criteria that it believes represents elements of a sharing framework and asked respondents to identify which best characterizes their current information-sharing framework. Table 10 shows that at all three levels of government, the sharing framework is incomplete, with cities—and small cities in particular—having few elements of a sharing framework operational.

Table 10: Survey Respondents Who Agreed That Elements of a Sharing Framework Exists by Answering “Great” to “Very Great”

Criteria	Percent			
	Federal agencies	States	Large cities	Small cities
Clear guidance for receiving from federal authorities	56	38	34	23
Clear guidance for providing to federal authorities	56	63	58	43
Clear and known process for receiving from federal authorities	81	45	46	33
Clear and known process for providing to federal authorities	63	60	62	47
Clearly defined person for receiving from federal	81	73	72	62
Clearly defined person for providing to federal	63	73	68	59
Clear what federal authorities should provide to you	38	38	25	22
Clear what you should provide to federal authorities	38	50	54	44
Information received from federal authorities is timely	38	38	23	14
Information provided to federal authorities is timely	56	68	62	48
Information received from federal authorities is accurate	31	48	39	21
Information provided to federal authorities is accurate	56	80	70	61
Information received from federal authorities is relevant	44	50	40	22
Information provided to federal authorities is relevant	56	58	60	39
Federal authorities give feedback when you share information with them	13	30	25	15
You give feedback when federal authorities share information with you	31	65	46	41
Have resources to analyze information received from federal authorities	31	40	42	33
Have the resources to analyze information to give to federal authorities	38	38	42	33
Routinely share information with federal authorities	69	65	60	36

**Appendix IV: Survey Responses to Our
Questions on the Elements of an Information-
Sharing Process That Are Already in Place**

Criteria	Percent			
	Federal agencies	States	Large cities	Small cities
Federal authorities routinely share information with you	56	28	22	10
You are involved early in federal investigations	13	25	25	22
Federal authorities are involved early in your investigations	13	38	45	30
Single credible source for receiving information/intelligence	13	35	32	30
Single credible source for receiving warnings and alerts	6	50	42	39
You have access to federal law enforcement databases	31	30	25	31
You have access to a secure, integrated Homeland Security database	19	25	12	20
You participate in national policy making process	38	25	8	7
Have clearance needed to access information	81	40	32	26
Can meet provisions to secure, maintain & destroy classified information	81	55	41	41

Source: GAO.

Note: Number of federal agency respondents = 16; number of state respondents = 40; number of large-city respondents = 106; and number of small-city respondents = 122.

Appendix V: Survey Responses to Perceived Barriers Faced by States/Cities in Providing the Federal Government with Information

We asked state, large-city and small-city respondents to identify what they perceive to be factors that hinder their organizations from providing federal authorities with homeland security information or intelligence. In contrast to the several barriers identified by federal respondents to providing state and local officials with information and intelligence, table 11 shows that states and city respondents identified the lack of integrated databases as the only significant barrier.

Table 11: Great to Very-Great Barriers to Providing Federal Authorities with Information and Intelligence

	Percent			
	Federal agencies	States	Large cities	Small cities
Legal barriers	13	3	4	3
Federal authorities' lack of interest in information to be provided	6	10	6	7
Culture of "information superiority"	6	3	4	5
Concerns about jeopardizing ongoing investigations	13	0	3	3
Lack of confidence in ability to limit disclosure of information	6	0	5	0
Lack of confidence in ability to manage investigations	6	0	3	0
Concerns about disclosing sources and methods	6	0	5	2
Lack of integration of databases	38	43	32	29

Source: GAO.

Note: Number of federal agency respondents = 16; number of state respondents = 40; number of large-city respondents = 106; and number of small-city respondents = 122.

Appendix VI: Comments from the Department of Homeland Security

38711

U.S. Department of Homeland Security

July 31, 2003

Raymond J. Decker
Director
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Decker:

Thank you for the opportunity to comment on your draft report, *HOMELAND SECURITY: Efforts to Improve Information Sharing Need to be Strengthened (GAO-03-760)*. We generally concur with the report and its recommendations. Information sharing is an essential tenet of the National Strategy for Homeland Security. Recognizing this need, our processes to share information with our many partners is a priority for the Department.

As you noted, most of your fieldwork was performed before the Department of Homeland Security (DHS) became operational in March 2003. Since the Department was created on January 24, 2003, and all of its component agencies and personnel reported to it on March 1, 2003, we have made significant strides to improve information sharing. For example, DHS is in the process of providing secure phones to the Governors and security clearances to the Homeland Security Advisors in every state so that relevant classified and other appropriate sensitive information can be shared. Even more important to the sharing of threat information with the state and local first responders who need it, however, is our increased focus on producing unclassified “tear-line” reporting whenever possible.

We note that much of the report is based on opinion data. We also note your footnote on page 21 that you “did not determine if these needs (for information) were valid.” We agree that “One reason that states and cities may not receive needed threat information is that the information may not be available.” This is often the case.

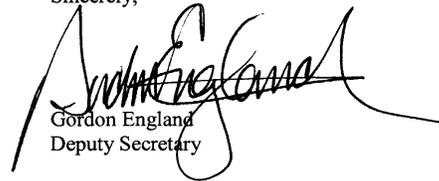
Not surprisingly, however, after just five months in operation, the Department is still formulating internal and external interfaces and protocols on many aspects of the complex issue of information sharing. The July 29, 2003, Executive Order on Homeland Security Information Sharing will assist us in these internal and external deliberations. We would caution that the difficulties of developing and rolling out a first draft of the national homeland security enterprise architecture with appropriate inter-agency coordination could go beyond the September 2003 target that was cited in the report. The

Washington, D. C. 20528

security considerations alone require a thoughtful, prudent and deliberate approach to this important issue.

We look forward to continuing a dialogue with you as we jointly cooperate to protect and defend America.

Sincerely,



Gordon England
Deputy Secretary

Appendix VII: Comments from the Department of Defense



INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

June 24, 2003

Mr. Raymond J. Decker
Director, Defense Capabilities and Management
U.S. General Accounting Office
Washington, DC 20548

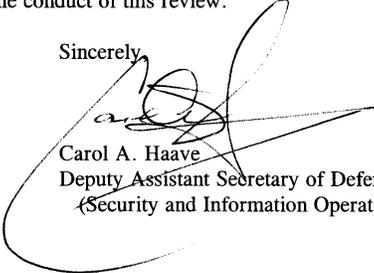
Dear Mr. Decker:

This is the Department of Defense (DoD) response to the GAO draft report, "HOMELAND SECURITY: Efforts to Improve Information Sharing Need to be Strengthened," dated May 27, 2003 (GAO Code 350240).

The DoD is in general agreement with the report as written. Specific comments are attached.

Thank you for the opportunity to respond to the GAO draft report and for the courtesies extended by your staff in the conduct of this review.

Sincerely,


Carol A. Haave
Deputy Assistant Secretary of Defense
(Security and Information Operations)

Enclosure: As stated



GAO DRAFT REPORT DATED MAY 27, 2003
GAO-03-760
(GAO CODE 350240)

"HOMELAND SECURITY: EFFORTS TO IMPROVE INFORMATION
SHARING NEED TO BE STRENGTHENED"

DEPARTMENT OF DEFENSE COMMENTS TO
THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommended that the Secretary of Homeland Security, in developing its enterprise architecture, work with the Attorney General of the United States, the Secretary of Defense, the Director of the Office of Management and Budget, the Director of the Central Intelligence Agency, and other appropriate federal, state and city authorities, and the private sector, to ensure that the enterprise architecture efforts incorporate the existing information-sharing guidance that is contained in the various national strategies and the information sharing procedures required by the Homeland Security Act to be established by the President. (p. 31/GAO Draft Report)

DOD RESPONSE: Concur

RECOMMENDATION 2: The GAO recommended that the Secretary of Homeland Security, in developing its enterprise architecture, work with the Attorney General of the United States, the Secretary of Defense, the Director of the Office of Management and Budget, the Director of the Central Intelligence Agency, and other appropriate federal, state and city authorities, and the private sector, to ensure that the enterprise architecture efforts establish a clearinghouse to coordinate the various information sharing initiatives to eliminate possible confusion and duplication of effort. (p. 31/GAO Draft Report)

DOD RESPONSE: Concur

RECOMMENDATION 3: The GAO recommended that the Secretary of Homeland Security, in developing its enterprise architecture, work with the Attorney General of the United States, the Secretary of Defense, the Director of the Office of Management and Budget, the Director of the Central Intelligence Agency, and other appropriate federal, state and city authorities, and the private sector, to ensure that the enterprise architecture efforts fully integrate states and cities in the national policy making process for information sharing and take steps to provide greater assurance that actions at all levels of government are mutually reinforcing. (p. 31/GAO Draft Report)

DOD RESPONSE: Concur

RECOMMENDATION 4: The GAO recommended that the Secretary of Homeland Security, in developing its enterprise architecture, work with the Attorney General of the United States, the Secretary of Defense, the Director of the Office of Management and Budget, the Director of the Central Intelligence Agency, and other appropriate federal, state and city authorities, and the private sector, to ensure that the enterprise architecture efforts identify and address the perceived barriers to federal information sharing. (p. 31/GAO Draft Report)

DOD RESPONSE: Concur

RECOMMENDATION 5: The GAO recommended that the Secretary of Homeland Security, in developing its enterprise architecture, work with the Attorney General of the United States, the Secretary of Defense, the Director of the Office of Management and Budget, the Director of the Central Intelligence Agency, and other appropriate federal, state and city authorities, and the private sector, to ensure that the enterprise architecture efforts include the use of survey methods or related data collection approaches to determine over time, the needs of private and public organizations for information related to homeland security and to measure progress in improving information sharing at all levels of government. (p. 31/GAO Draft Report)

DOD RESPONSE: Concur

Appendix VIII: Comments from the Department of Justice



U.S. Department of Justice

Washington, D.C. 20530

June 25, 2003

Raymond J. Decker
Director, Diffuse Threats Issues
Defense Capabilities and Management
U.S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Decker:

On May 27, 2003, you provided the Department of Justice (DOJ) with a copy of the General Accounting Office (GAO) draft report entitled "HOMELAND SECURITY: Efforts to Improve Information Sharing Needs to be Strengthened" (GAO 03-760/350240), with a request for comments by June 25, 2003. We appreciate the opportunity to review the draft report.

The draft report reaches sweeping and extraordinarily negative conclusions about the adequacy of the governmental sharing of information in order to prevent acts of terrorism. We believe that these conclusions are fundamentally incorrect and unsupported by reliable evidence. A critical element in any valid evaluation of government information sharing for homeland security purposes is a review of the adequacy of intelligence sharing. As we previously advised GAO staff, however, the review of intelligence activities is an arena that is beyond GAO's purview. For this reason, we declined to provide GAO with information on intelligence sharing. Additionally, we understand that the draft report relies substantially upon information from a survey of agency views. However, for reasons that we also discussed with GAO staff, neither this Department nor the Central Intelligence Agency participated in that survey.

To assist Congress in fulfilling its oversight responsibilities, the executive branch regularly provides information and briefings to the congressional intelligence committees, and on occasion to other committees, including information about intelligence sharing within the federal government and with state and local officials. To provide information on intelligence sharing to GAO, however, would represent a departure from the long-standing practice of Congress and the executive branch regarding the oversight

Mr. Raymond J. Decker

Page 2

of intelligence activities. Although as a result of this long-standing practice GAO may not be able to present the Congress with useful information on the intelligence activities of the executive branch, we are confident that Congress is receiving directly sufficient information on these activities to make informed decisions on the budget and other legislation.

If you have any questions concerning the Department's comments in this matter, please feel free to contact Vickie L. Sloan, Director, Audit Liaison Office, Justice Management Division on (202) 514-0469.

Sincerely,

A handwritten signature in black ink, appearing to read "P R Corts", with a long horizontal stroke extending to the right.

Paul R. Corts
Assistant Attorney General
for Administration

Appendix IX: GAO Contacts and Staff Acknowledgments

GAO Contacts

Raymond J. Decker (202) 512-6020
Brian J. Lepore (202) 512-4523

Acknowledgments

In addition to those named above, Lorelei St. James, Patricia Sari-Spear, Tinh Nguyen, Rebecca Shea, Adam Vodraska, and R.K. Wild made key contributions to this report.

Related GAO Products

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

Combating Terrorism: Observations on National Strategies Related to Terrorism. [GAO-03-519T](#). Washington, D.C.: March 3, 2003.

Homeland Security: Effective Intergovernmental Coordination Is Key to Success. [GAO-02-1013T](#). Washington, D.C.: August 23, 2002.

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

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

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

FBI Intelligence Investigations: Coordination within Justice on Counterintelligence Criminal Matters Is Limited. [GAO-01-780](#). Washington, D.C.: July 16, 2001.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

E-mail: fraudnet@gao.gov

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

Public Affairs

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