United States General Accounting Office

GAO

Testimony

Before the Senate Committee on Governmental Affairs

For Release on
Delivery Expected at
9:30 a.m., EDT
Friday
September 21, 2001

HOMELAND SECURITY

A Framework for Addressing the Nation's Efforts

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

Mr. Chairman and Members of the Committee:

We at GAO, along with all Americans, were shocked and saddened by the coordinated terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001. The events of that day remind us that terrorism victimizes real people—men, women, and children—our families, friends, neighbors, and colleagues. Our hearts go out to the families of the victims of the attack and to the families of the heroic rescue crews, those responders who were lost trying to save others. They and many other responders have served with distinction and valor.

I appreciate the opportunity to discuss with you today a framework for addressing federal efforts to provide for homeland security. I would like to address the issue by making three points. First, I will discuss the nature of the threats that face the United States today. Second, I will offer some thoughts on what government could do to both counter the threats and provide for a more secure homeland. Third, I will offer a framework for how the government might organize a homeland security program. We have completed work in a variety of areas related to homeland security, and I will reiterate some of our major recommendations from this work.

Summary

According to a variety of U.S. intelligence assessments, the United States now confronts a range of increasingly diffuse threats that puts greater destructive power into the hands of small states, groups, and individuals and threatens our values and way of life. These threats range from incidents of terrorism and information attacks on critical infrastructure to the potential use of weapons of mass destruction and the spread of infectious diseases. Each one of these threats could cause massive casualties and disruption.

Our work indicates that in efforts of this kind—which involve many federal agencies as well as state and local governments, the private sector, and private citizens—the federal government must address three fundamental needs. First, the government needs clearly defined and effective leadership with a clear vision to develop and implement a homeland security strategy in coordination with all relevant partners, and the ability to marshal the necessary resources to get the job done. Second, a national homeland security strategy should be developed based on a comprehensive assessment of national threats and risks. Third, the large number of organizations that will be involved in homeland security need to have clearly articulated roles, responsibilities, and accountability mechanisms.

Crafting a strategy for homeland security involves reducing the risk where possible, assessing the nation's vulnerabilities, and identifying the critical infrastructure most in need of protection. To be comprehensive, the strategy should include steps to use intelligence assets or other means to identify attackers and prevent attacks before they occur, harden potential targets to minimize the damage from an attack, and effectively manage the consequences of an incident. In addition, the strategy should focus resources on areas of greatest need and measure performance against strategic goals. Because the plan will need to be executed nationally, the federal government can assign roles to federal agencies once the strategy is developed, but also will need to develop cooperative partnerships with state and local governments as well as with the private and not-for-profit sectors. Effective homeland security also will require forming international partnerships to identify attackers, prevent attacks, and retaliate if there are any attacks.

The Nature of the Threat Facing the United States

As we noted in GAO's strategic plan, the United States and other nations face increasingly diffuse threats. In the future, potential adversaries are more likely to strike vulnerable civilian or military targets in nontraditional ways to avoid direct confrontation with our military forces on the battlefield. The President's December 2000 national security strategy states that porous borders, rapid technological change, greater information flow, and the destructive power of weapons now within the reach of small states, groups, and individuals make such threats more viable and endanger our values, way of life, and the personal security of our citizens.

Hostile nations, terrorist groups, transnational criminals, and even individuals may target American people, institutions, and infrastructure with weapons of mass destruction and outbreaks of infectious disease. They may attempt to disrupt or destroy our information systems through cyber warfare. International criminal activities such as money laundering, arms smuggling, and drug trafficking can undermine the stability of social and financial institutions and the health of our citizens. As we witnessed in the tragic events of last week, some of the emerging threats can produce mass casualties. Others can lead to mass disruption of critical infrastructure and can hold serious implications for both our domestic and the global economy, as we saw when the New York Stock Exchange re-opened for trading this past Monday and the Dow Jones Industrial Average fell more than 600 points. Terrorist attacks also could compromise the integrity or delivery of water or electricity to our citizens, compromise the safety of the traveling public, and undermine the soundness of government and commercial data systems supporting a myriad of activities.

A basic and fundamental role of the government under our Constitution is to protect America from both foreign and domestic threats. The government must be able to prevent and deter threats to our homeland as well as detect impending danger before attacks or incidents occur. However, it may not be possible to prevent, deter, and detect every threat, so steps should be taken to harden potential targets. We also must be ready to manage the crises and consequences of an event, to treat casualties, reconstitute damaged infrastructure, and move the nation forward. Finally, the government must be prepared to retaliate against the responsible parties in the event of an attack.

What Government Could Do to Address Homeland Security

Now I would like to turn to what the government could do to make our homeland more secure. First, I will discuss the need for clearly defined and effective leadership with a clear vision of what needs to be accomplished. Second, I will address the need for a coordinated national strategy and comprehensive threat assessment.

A Focal Point Is a Critical Component of Homeland Security Strategy

Yesterday, we issued a report that discusses challenges confronting policymakers in the war on terrorism and offered a series of recommendations. One of these recommendations is that the government needs more clearly defined and effective leadership to develop a strategy for combating terrorism, to oversee development of a new national threat and risk assessment, and to coordinate implementation among federal agencies. Similar leadership also is needed to address the broader issue of homeland security. Specifically, a national focal point will be critical to articulate a vision for ensuring the security of the American homeland and to develop and implement a strategy to realize that vision. The entity that functions as the focal point should be dedicated to this function. In addition, the person who heads this entity should be dedicated full-time to this effort and consideration should be given to a term appointment in order to enhance continuity.

In testimony on March 27, 2001, we stated that overall leadership and management efforts to combat terrorism are fragmented because there is no single focal point managing and overseeing the many functions conducted by more than 40 different federal departments and agencies.[1] Also, our past work in combating terrorism has shown that the multitude of federal programs requires focus and attention to minimize redundancy

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

of effort and eliminate confusion within the federal government and at the state and local level. Homeland security will rely on the concerted efforts of scores of agencies, which may exceed the number in the fight against terrorism. Consequently, the need for overall leadership is even more critical.

At present, we do not have a national strategy specifically for ensuring homeland security. Thus, the strategy must establish the parameters of homeland security and contain explicit goals and objectives. It will need to be developed in partnership with Congress, the executive branch, state and local governments, and the private sector (which owns much of the critical infrastructure that can be targeted). Without such a strategy, efforts may be fragmented and cause confusion, duplication of effort, and ineffective alignment of resources with strategic goals. Consequently, clarifying the roles and responsibilities of the various levels of government and the private sector will be a critical function for the entity that is given oversight responsibility for homeland security efforts.

The Country Needs a Comprehensive National Security Threat and Risk Assessment

The United States does not have a national threat and risk assessment to help guide federal programs for homeland security. A threat and risk assessment is a decision-making tool that helps to define the threats, to evaluate the associated risk, and to link requirements to program investments. In our March 2001 testimony on combating terrorism, we stated that an important first step in developing a strategy for combating terrorism is to conduct a national threat and risk assessment to define and prioritize requirements. Combating terrorism is a major component of homeland security, but it is not the only one. It is essential that a national threat and risk assessment be undertaken that will address the full range of threats to the homeland.

Results from hearings and other studies also underscore the importance of a national threat and risk assessment. For example, in a July 2001 letter to the vice president from several senators, the senators stated that federal programs to combat domestic terrorism are being initiated and expanded without the benefit of a sound national threat and risk assessment process.[2] In a May 2001 Center for Strategic and International Studies' report on homeland defense, the authors stated that an annual threat assessment would provide federal planners with the basis for assessing the

[2] *Report to the Vice-President: Findings Pursuant to the Senate Hearings on US Federal Government Capabilities to Combat Domestic Terrorism* (July 13, 2001).

emerging risk of attacks and developing an integrated analysis structure for planning.[3]

We recognize that a national-level threat and risk assessment will not be a panacea for all the problems in providing homeland security. However, we believe that such a national threat and risk assessment could provide a framework for action and facilitate multidisciplinary and multi-organizational participation in planning, developing, and implementing programs to enhance the security of our homeland. Given the tragic events of Tuesday, September 11, 2001, a comprehensive national-level threat and risk assessment that addresses all threats has become an urgent imperative.

How the Country Should Develop the National Strategy

Now, I would like to discuss some elements that may need to be included in the development of the national strategy and a means to assign roles to federal, state, and local governments and the private sector.

Three essential elements provide a basis for developing a national strategy: a risk assessment, vulnerability analysis, and infrastructure criticality analysis. This approach, developed by the Department of Defense for its antiterrorism program, could be an instructive model in developing a homeland security strategy. First, our nation must thoroughly assess the threats posed by nations, groups, or individuals and, to the extent possible, eliminate or reduce the threat. Second, we have to identify the vulnerabilities and weaknesses that exist in our infrastructure, operations, planning, and exercises and then identify steps to mitigate those risks. Third, we must assure our ability to respond to and mitigate the consequences of an attack. Given time and resource limitations, we must identify the most critical aspects of our infrastructure and operations that require the most immediate attention.

Our strategy, to be comprehensive in nature, should include steps designed to

- reduce our vulnerability to threats, for example, by hardening targets to minimize the damage from an attack;

[3] *Combating Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Strategy* (Report of the CSIS Homeland Defense Project, May 2001).

- use intelligence assets to identify threats;
- stop attacks before they occur; and
- manage the consequences of an incident.

In addition, the strategy should incorporate mechanisms to assess resource utilization and program performance as well as provide for training, exercises, and equipment to respond to tragic events such as those that occurred last week. Because we may not be able to eliminate all vulnerabilities within our borders, prevent all threat activity, or be completely prepared to respond to all incidents, our strategy should focus finite national resources on areas of greatest need.

Once a strategy is developed, all levels of government and the private sector will need to understand and prepare for their defined roles under the strategy. While the federal government can assign roles to federal agencies under the strategy, it will need to reach consensus with the other levels of government and with the private sector on their roles.

In the 1990s, the world was concerned about the potential for computer failures at the start of the new millennium, an issue that came to be known as Y2K. The Y2K task force approach may offer a model for developing the public-private partnerships necessary under a comprehensive homeland security strategy. A massive mobilization with federal government leadership was undertaken in connection with Y2K which included partnerships with the private sector and international governments and effective communication to implement any needed corrections. The value of federal leadership, oversight, and partnerships was repeatedly cited as a key to success in addressing Y2K issues at a Lessons Learned summit held last year. Developing a homeland security plan may require a similar level of leadership, oversight, and partnerships with nearly every segment of American society—including individual U.S. citizens—as well as with the international community. In addition, as in the case of our Y2K efforts, Congress needs to take an active, ongoing, and crosscutting approach to oversight in connection with the design and implementation of the homeland security strategy.

Prior GAO Work Related to Homeland Security

We at GAO have completed several congressionally requested efforts on numerous topics related to homeland security. I would like to briefly summarize some of the work that we have done in the areas of combating terrorism, aviation security, transnational crime, protection of critical infrastructure, and public health.

Combating Terrorism

Given concerns about the preparedness of the federal government and state and local emergency responders to cope with a large-scale terrorist attack involving the use of weapons of mass destruction, we have reviewed the plans, policies, and programs for combating domestic terrorism involving weapons of mass destruction. Our report, *Combating Terrorism: Selected Challenges and Related Recommendations*,[4] was issued yesterday and updates our extensive evaluations in recent years of federal programs to combat domestic terrorism and protect critical infrastructure.

Progress has been made since we first began looking at these issues in 1995. Interagency coordination has improved, and interagency and intergovernmental command and control now is regularly included in exercises. Agencies also have completed operational guidance and related plans. Federal assistance to state and local governments to prepare for terrorist incidents has resulted in training for thousands of first responders, many of whom went into action at the World Trade Center and at the Pentagon on September 11, 2001.

However, some key elements remain incomplete. As a result, we recommended that the President designate a single focal point with responsibility and authority for all critical functions necessary to provide overall leadership and coordination of federal programs to combat terrorism. The focal point should oversee a national-level threat assessment on likely weapons of mass destruction that might be used by terrorists and lead the development of a national strategy to combat terrorism and oversee its implementation. Furthermore, we recommended that the Assistant to the President for Science and Technology complete a strategy to coordinate research and development to improve federal capabilities and avoid duplication.

[4] *Combating Terrorism: Selected Challenges and Related Recommendations* (GAO-01-822, Sept. 20, 2001).

Aviation Security

Now let me turn to aviation security. Since 1996, we have presented numerous reports and testimonies and reported on numerous weaknesses that we found in the commercial aviation security system. For example, we reported that airport passenger screeners do not perform well in detecting dangerous objects, and Federal Aviation Administration tests showed that as testing gets more realistic—that is, as tests more closely approximate how a terrorist might attempt to penetrate a checkpoint—screener performance declines significantly. In addition, we were able to penetrate airport security ourselves by having our investigators create fake credentials from the Internet and declare themselves law enforcement officers. They were then permitted to bypass security screening and go directly to waiting passenger aircraft. In 1996, we outlined a number of steps that required immediate action, including identifying vulnerabilities in the system; developing a short-term approach to correct significant security weaknesses; and developing a long-term, comprehensive national strategy that combines new technology, procedures, and better training for security personnel.

Cyber Attacks on Critical Infrastructure

Federal critical infrastructure-protection initiatives have focused on preventing mass disruption that can occur when information systems are compromised because of computer-based attacks. Such attacks are of growing concern due to the nation's increasing reliance on interconnected computer systems that can be accessed remotely and anonymously from virtually anywhere in the world. In accordance with Presidential Decision Directive 63, issued in 1998, and other information-security requirements outlined in laws and federal guidance, an array of efforts has been undertaken to address these risks. However, progress has been slow. For example, federal agencies have taken initial steps to develop critical infrastructure plans, but independent audits continue to identify persistent, significant information security weaknesses that place virtually all major federal agencies' operations at high risk of tampering and disruption. In addition, while federal outreach efforts have raised awareness and prompted information sharing among government and private sector entities, substantive analysis of infrastructure components to identify interdependencies and related vulnerabilities has been limited. An underlying deficiency impeding progress is the lack of a national plan that fully defines the roles and responsibilities of key participants and establishes interim objectives. Accordingly, we have recommended that the Assistant to the President for National Security Affairs ensure that the government's critical infrastructure strategy clearly define specific roles and responsibilities, develop interim objectives and milestones for achieving adequate protection, and define performance measures for accountability. The administration currently is reviewing and considering

adjustments to the government's critical infrastructure-protection strategy that may address this deficiency.

International Crime Control

On September 20, 2001, we publicly released a report on international crime control and reported that individual federal entities have developed strategies to address a variety of international crime issues, and for some crimes, integrated mechanisms exist to coordinate efforts across agencies. However, we found that without an up-to-date and integrated strategy and sustained top-level leadership to implement and monitor the strategy, the risk is high; scarce resources will be wasted; overall effectiveness will be limited or not known; and accountability will not be ensured. We recommended that the Assistant to the President for National Security Affairs take appropriate action to ensure sustained executive-level coordination and assessment of multiagency federal efforts in connection with international crime. Some of the individual actions we recommended were to update the existing governmentwide international crime threat assessment, to update or develop a new International Crime Control Strategy to include prioritized goals as well as implementing objectives, and to designate responsibility for executing the strategy and resolving any jurisdictional issues.

Public Health

The spread of infectious diseases is a growing concern. Whether a disease outbreak is intentional or naturally occurring, the public health response to determine its causes and contain its spread is the same. Because a bioterrorist event could look like a natural outbreak, bioterrorism preparedness rests in large part on public health preparedness. In our review last year of the West Nile virus outbreak in New York, we found problems related to communication and coordination among and between federal, state, and local authorities. Although this outbreak was relatively small in terms of the number of human cases, it taxed the resources of one of the nation's largest local health departments. In 1999, we reported that surveillance for important emerging infectious diseases is not comprehensive in all states, leaving gaps in the nation's surveillance network. Laboratory capacity could be inadequate in any large outbreak, with insufficient trained personnel to perform laboratory tests and insufficient computer systems to rapidly share information. Earlier this year, we reported that federal agencies have made progress in improving their management of the stockpiles of pharmaceutical and medical supplies that would be needed in a bioterrorist event, but that some problems still remained. There are also widespread concerns that hospital emergency departments generally are not prepared in an organized fashion to treat victims of biological terrorism and that hospital emergency capacity is already strained, with emergency rooms in major metropolitan

areas routinely filled and unable to accept patients in need of urgent care. To improve the nation's public health surveillance of infectious diseases and help ensure adequate public protection, we recommended that the Director of the Centers for Disease Control and Prevention lead an effort to help federal, state, and local public health officials achieve consensus on the core capacities needed at each level of government. We advised that consensus be reached on such matters as the number and qualifications of laboratory and epidemiological staff as well as laboratory and information technology.

Conclusion

Based on the tragic events of last week and our observations over the past several years, there are several key questions that need to be asked in addressing homeland security:

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

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

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

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

Homeland security issues are now at the top of the national agenda, as a result of last week's tragic events. As a result, it is clear that the administration has taken and is taking a variety of actions to identify responsible parties for last week's attacks, manage the related consequences and mitigate future risks. Obviously, we have not been able to assess the nature and extent of this effort in the wake of last week's events. We expect that we will be asked to do so in due course.

Finally, Mr. Chairman, as you might expect, we have been inundated with requests to brief congressional committees and members on our present and pending work and to undertake new work. We are working with the congressional leadership to be sure we have focused our limited resources on the most important issues. We look forward to working with you and

others to focus our work and to identify options for how best to proceed while holding responsible parties accountable for desired outcomes. This concludes my prepared statement.

I would be happy to answer any questions that you may have.