Strategic Objective:

Respond to Diffuse Threats to National and Global Security

Issue: The United States and other nations face increasingly diffuse threats in the post–cold war era. Adversaries have demonstrated they are more likely to strike vulnerable civilian or military targets in nontraditional ways to avoid direct confrontation with U.S. military forces on the battlefield. Porous borders and rapid technological change make such threats more viable. At risk are the nation's values, way of life, and the personal security of its citizens.

In response to the most recent attacks, the President, on October 8, 2001, established the Office of Homeland Security to develop and coordinate a national strategy. The office will coordinate the nation's efforts to prevent, respond, and recover from the aftermath of terrorist attacks and to plan and budget for its homeland security mission. To support this new strategy, there also will have to be a concerted effort to improve the threat information the United States receives from foreign and domestic sources; to understand the nature of the threats to vulnerable assets and processes; and to protect the nation's military forces, critical infrastructures and computer and telecommunications systems, and population. As discussed earlier, preparing and responding to these threats will entail a governmentwide effort involving both defense and domestic agencies and programs. Internationally, the United States and its allies will have to bolster their efforts to prevent the proliferation of dangerous weapons that can be used to carry out threats to the nation's security.

Performance Goals: To support congressional and federal decision making on governmentwide preparation for and response to diffuse threats to national and global security, GAO will

- analyze the effectiveness of the federal government's approach to providing for homeland security;
- assess U.S. efforts to protect computer and telecommunications systems supporting critical infrastructures in business and government; and
- assess the effectiveness of U.S. and international efforts to prevent the proliferation of nuclear, biological, chemical, and conventional weapons and sensitive technologies.

Analyze the Effectiveness of the Federal Government's Approach to Providing for Homeland Security

Key Efforts

- ❑ Evaluate the Office of Homeland Security's efforts to institutionalize and sustain the homeland security effort over the long term, including the ability to influence budget and resource allocations, prioritize programs, and coordinate roles and responsibilities across numerous agencies and all levels of government
- ❑ Evaluate the risk management approach that underpins the strategies being developed to improve homeland security and related resource allocations
- ❑ Evaluate the capability of all levels of government to respond to and mitigate the consequences of threats to homeland security
- ❑ Assess offensive measures taken by federal agencies to detect, prevent, or deter terrorist attacks or naturally occurring disasters
- ❑ Examine federal, state, and local government homeland security efforts to identify best practices and enhance intergovernmental coordination and effective resource utilization
- ❑ Evaluate the threat analysis and linguistic support capabilities of intelligence organizations and the extent to which intelligence information is provided to federal, state, and local authorities
- ❑ Evaluate U.S. forces protection measures, including capabilities to defend against chemical and biological warfare

Significance

The September 11 terrorist attacks have highlighted the need to improve the national security strategy of the United States to prevent catastrophic incidents that threaten the homeland or to adequately respond if they do occur. At the same time, naturally occurring catastrophes, such as the outbreak of infectious diseases, could also threaten the homeland. Virtually every federal agency, state, locality, private sector entity, and citizen has a role in homeland security. Consequently, planning for and coordinating the homeland security efforts of the public and private sectors is a major and urgent challenge for the federal government. In addition, U.S. military forces at home and abroad also face diffuse threats and weapons of mass destruction that could be used to avoid direct confrontation on a conventional battlefield and cause substantial casualties and loss of life.

A fundamental role of the federal government under the guidance of the recently established Office of Homeland Security is to protect America and its citizens from both foreign and domestic threats. The combined efforts of government agencies must be designed to prevent and deter threats to the homeland and U.S. interests abroad as well as to detect impending danger before attacks or incidents occur. The government also must be ready to manage the crises and consequences of an event by treating casualties, reconstituting damaged infrastructure, and moving the nation forward. Finally, the government must be prepared to retaliate against the responsible parties in the event of an attack. To accomplish this role and address the new priority on homeland security, several critical elements must be put in place. This performance goal addresses the overall homeland security strategy. Other performance goals address specific elements of the strategy, including protection of the transportation sector, computer information and telecommunications systems, and the Department of Defense's (DOD) battlefield information capabilities. Managing the risks of terrorism and prioritizing the application of resources to the homeland security effort will require a careful assessment of the threats the nation faces, the vulnerabilities, and the criticality of the infrastructure that support U.S. interests.

Analyze the Effectiveness of the Federal Government's Approach to Providing for Homeland Security (cont.)

- ❑ Review DOD's chemical demilitarization program to determine if the program can meet international commitments and if security and emergency preparedness is sufficient to guarantee the public's safety

Potential Outcomes that Could Result when GAO's Work Is Used

Improved effectiveness of the Office of Homeland Security to develop, implement, and sustain a long-term homeland security strategy

Improved effectiveness of the nation's homeland security strategy and resource allocations

Improved preparedness of the federal, state, and local governments to respond to a terrorist attack and ensure that federal funding is used effectively

Improved U.S. ability to prevent attacks before they occur

Enhanced ability of the three levels of government to coordinate their intelligence collection, planning, and execution of homeland security missions

Improved U.S. ability to identify threats and provide advance indications and warning of an impending attack to all organizations responsible for homeland security

Improved chemical and biological defenses for U.S. military forces

Increased congressional understanding of the status of the Army's execution of the program to destroy the nation's stockpile of chemical weapons and the preparedness of communities near the stockpile to respond to a chemical accident

Assess U.S. Efforts to Protect Computer and Telecommunications Systems Supporting Critical Infrastructures in Business and Government

Key Efforts

- ❑ Assess computer security controls associated with critical federal systems
- ❑ Evaluate computer security processes of unique or high-risk federal government applications, such as Social Security
- ❑ Assess federal efforts to establish and promote public-private partnerships to reduce the threat of cyber attacks
- ❑ Provide assistance to the Congress in identifying potential changes to computer security legislation
- ❑ Assess the government's efforts to limit fraudulent activity such as credit card fraud over the Internet
- ❑ Evaluate federal efforts to facilitate development of standards for communications among computers over the Internet to make it easier to conduct electronic government
- ❑ Assess federal efforts to develop and implement governmentwide improvements to computer security and critical infrastructure protection initiatives
- ❑ Assess the effectiveness of public and private sector efforts to protect the nation's telecommunication infrastructure

Significance

Protection of the nation's critical infrastructure—including that for energy, financial services, transportation, vital human services, and communications systems—is becoming increasingly important due largely to the dependence on complex interconnected computer and telecommunications systems. Criminals, terrorists, and others, working anonymously from remote locations and with relatively limited resources, can now use computers and the open interconnectivity of the Internet to severely disrupt this infrastructure, which is essential to national defense, economic prosperity, and quality of life. Similar means can be used to commit massive fraud and gain access to highly sensitive information. In response, new laws such as government information security reform and presidential initiatives such as Presidential Decision Directive 63 and Executive Order 13231 have prompted an array of federal efforts aimed at improving critical infrastructure protection, especially information security, in both the public and private sectors. These efforts have also raised a variety of policy and budgetary issues that will need to be addressed as government works with the private sector to develop an effective strategy for protecting against computer-based attacks.

Potential Outcomes that Could Result when GAO's Work Is Used

Reasonable assurance that critical operations are protected from disruption, fraud, and misuse

Enhanced capability of organizations to detect, protect against, and respond to computer intrusions

Greater coordination among public and private sector institutions in protecting U.S. computer-based critical infrastructure systems

Improvements to the legislative framework for information security

Greater public assurance that Internet, electronic commerce transactions, and the nation's telecommunication infrastructure are secure

More secure and efficient electronic government operations

Assess the Effectiveness of U.S. and International Efforts to Prevent the Proliferation of Nuclear, Biological, Chemical, and Conventional Weapons and Sensitive Technologies

Key Efforts

- ❑ Evaluate the management and effectiveness of executive branch efforts to minimize the proliferation of former Soviet nuclear, chemical, and biological assets that pose the greatest risk to the United States
- ❑ Assess the effectiveness of U.S. and multilateral controls over exports of goods and technologies that could help proliferate weapons of mass destruction or destabilizing conventional weapons to sensitive regions of the world
- ❑ Evaluate the impacts of accords aimed at managing or reducing national arsenals of weapons of mass destruction

Significance

The continuing proliferation of weapons of mass destruction and delivery systems poses serious threats to the security of the United States. The danger that, in the near future, a rogue regime or terrorists will be able to threaten the United States or its allies with nuclear, chemical, or biological weapons has led the United States to initiate a variety of programs aimed at preventing such an outcome. For example, DOD's Cooperative Threat Reduction Program is now the centerpiece of a growing multibillion-dollar array of efforts by the Departments of Defense, Energy, and State to help former Soviet states control and reduce their vast, diverse holding of cold war–era nuclear, chemical, and biological weapons and their related delivery systems and infrastructure. These efforts must overcome numerous obstacles in the former Soviet states, including a precipitous decline in Russia's economy that has led the United States to assume an increasing share of the cost of controlling former Soviet weapons of mass destruction. U.S. efforts must therefore focus on the former Soviet assets that pose the greatest risks and effectively reduce those risks. In addition, the United States controls the export of certain sensitive technologies (such as chemical weapons precursors, missiles, and computers) and weapons systems. The United States has entered into several export control agreements with other nations capable of supplying these technologies or weapons systems. However, because such controls can be weakened by the pace of technological advances, by a changing consensus about what technologies to restrict and how to restrict them, and by efforts of countries of concern to circumvent controls, the United States is seeking ways to strengthen multilateral export control regimes. Finally, the United States is reassessing the effect of existing agreements to control or reduce U.S. and foreign arsenals of weapons of mass destruction in the post–cold war era, as well as the ability of prospective agreements to effectively prohibit and detect development of weapons of mass destruction.

Potential Outcomes that Could Result when GAO's Work Is Used

Improved management of programs and increased focus on former Soviet assets that pose the greatest risks to U.S. national security

Enhanced controls over the export of sensitive technologies that could facilitate the proliferation of weapons of mass destruction or other weapons of concern

Assess the Effectiveness of U.S. and International Efforts to Prevent the Proliferation of Nuclear, Biological, Chemical, and Conventional Weapons and Sensitive Technologies (cont.)

Analyses of efforts to implement accords to help the Congress identify areas needing improvement and oversight