United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Cybersecurity, Science, and Research and Development and the Subcommittee on Infrastructure and Border Security, Select Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 3:00 p.m. EDT
Wednesday, September 17, 2003

HOMELAND SECURITY

Information Sharing Responsibilities, Challenges, and Key Management Issues

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-03-1165T

September 17, 2003

HOMELAND SECURITY

Information Sharing Responsibilities, Challenges, and Key Management Issues

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-1165T, a testimony before the Subcommittee on Cybersecurity, Science, and Research and Development and the Subcommittee on Infrastructure and Border Security, Select Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The Homeland Security Act of 2002, which created the Department of Homeland Security (DHS), brought together 22 diverse organizations to help prevent terrorist attacks in the United States, reduce the vulnerability of the United States to terrorist attacks, and minimize damage and assist in recovery from attacks that do occur. To accomplish this mission, the act established specific homeland security responsibilities for the department, which included sharing information among its own entities and with other federal agencies, state and local governments, the private sector, and others.

GAO was asked to discuss the significance of information sharing in fulfilling DHS's responsibilities, emphasizing GAO's related prior analyses and recommendations for improving the federal government's information sharing efforts.

What GAO Found

DHS's responsibilities include coordinating and sharing information related to threats of domestic terrorism within the department and with and between other federal agencies, state and local governments, the private sector, and other entities. To accomplish its missions, DHS must, for example, access, receive, and analyze law enforcement information, intelligence information, and other threat, incident, and vulnerability information from federal and nonfederal sources and analyze such information to identify and assess the nature and scope of terrorist threats. DHS must also share information both internally and externally with agencies and law enforcement on such things as goods and passengers inbound to the United States and individuals who are known or suspected terrorists and criminals.

GAO has made numerous recommendations related to information sharing particularly as they relate to fulfilling DHS's critical infrastructure protection responsibilities. Although improvements have been made, more efforts are needed to address the following challenges, among others, that GAO has identified:

- developing a comprehensive and coordinated national plan to facilitate information sharing on critical infrastructure protection;
- developing productive information sharing relationships between the federal government and state and local governments and the private sector; and
- providing appropriate incentives for nonfederal entities to increase information sharing with the federal government and enhance other critical infrastructure protection efforts.

Through our prior work, we have identified critical success factors and other key management issues that DHS should consider as it establishes systems and processes to facilitate information sharing among and between government entities and the private sector. These success factors include establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents. Further, as part of its information technology management, DHS should continue to develop and implement an enterprise architecture to integrate the many existing systems and processes required to support its mission and to guide the department's investments in new systems to effectively support homeland security in the coming years. Other key management issues include ensuring that sensitive information is secured, developing secure communications networks, integrating staff from different organizations, and ensuring that the department has properly skilled staff.

www.gao.gov/cgi-bin/getrpt?GAO-03-1165T.

To view the full testimony, click on the link above.
For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

Messrs. Chairmen and Members of the Subcommittees:

I am pleased to be here today to discuss the challenges that the Department of Homeland Security (DHS) faces in integrating its information gathering and sharing functions, particularly as they relate to fulfilling their critical infrastructure protection (CIP) responsibilities. CIP involves activities that enhance the security of the cyber and physical public and private infrastructures that are essential to our national security, national economic security, and/or national public health and safety. The Homeland Security Act of 2002 brought together 22 diverse organizations and created DHS to help prevent terrorist attacks in the United States, reduce the vulnerability of the United States to terrorist attacks, and minimize damage and assist in recovery from attacks that do occur. To accomplish this mission, the act established specific homeland security and CIP responsibilities for the department and directed it to coordinate its efforts and share information among its own entities and with other federal agencies, state and local governments, the private sector, and others.

In my testimony today, I will summarize our analysis of information sharing as an integral part of fulfilling DHS's mission and CIP responsibilities. I will then discuss our related prior analyses and recommendations for improving the federal government's information sharing efforts. Last, I will discuss the key management issues that DHS should consider in developing and implementing effective information sharing processes and systems.

In preparing this testimony, we relied on prior GAO reports and testimonies on combating terrorism, critical infrastructure protection (CIP), homeland security, information sharing, information technology (IT), and national preparedness, among others. These prior reports and testimonies included our review and analysis of the *National Strategy for Homeland Security*, the *National Strategy to Secure Cyberspace*, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, the *National Strategy for Combating Terrorism*,[1] the Homeland Security Act of 2002,[2] and other relevant federal policies. Our work for today's testimony was performed in September 2003 in accordance with generally accepted government auditing standards.

[1]The White House, *The National Strategy for Homeland Security* (Washington, D.C.: July 2002); *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003); *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: February 2003); and *The National Strategy for Combating Terrorism* (Washington, D.C.: February 2003).
[2]Public Law 107-296.

Results in Brief

The Homeland Security Act of 2002 and other federal policy, including the *National Strategy for Homeland Security*, assign responsibilities to DHS for coordinating and sharing information related to threats of domestic terrorism, within the department and with and between other federal agencies, state and local governments, the private sector, and other entities. For example, to accomplish its missions, the new department must (1) access, receive, and analyze law enforcement information, intelligence information, and other threat, incident, and vulnerability information from federal and nonfederal sources; (2) analyze this information to identify and assess the nature and scope of terrorist threats; and (3) administer the Homeland Security Advisory System and provide specific warning information and advice on appropriate protective measures and countermeasures. Further, DHS must share information both internally and externally with agencies and law enforcement on such things as goods and passengers inbound to the United States and individuals who are known or suspected terrorists and criminals. It also must share information among emergency responders in preparing for and responding to terrorist attacks and other emergencies.

We have made numerous recommendations over the last several years related to information sharing functions that have been transferred to DHS. One significant area concerns the federal government's CIP efforts, which is focused on 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. Although improvements have been made, further efforts are needed to address the following critical CIP challenges:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;
- developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector;
- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely, useful warnings and other information concerning

both cyber and physical threats to federal entities, state and local governments, and the private sector; and

- providing appropriate incentives for nonfederal entities to increase information sharing with the federal government and enhance other CIP efforts.

In addition, we recently identified challenges in consolidating and standardizing watch list structures and policies, which are essential to effectively sharing information on suspected terrorists and criminals.[3]

The success of homeland security also relies on establishing effective systems and processes to facilitate information sharing among and between government entities and the private sector. Through our prior work, we have identified critical success factors and other key management issues that DHS should consider as it establishes systems and processes to facilitate information sharing among and between government entities and the private sector. These success factors include establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents. As part of its information technology management, DHS should continue to develop and implement an enterprise architecture to integrate the many existing systems and processes required to support its mission and to guide the department's investments in new systems to effectively support homeland security in the coming years. Other key management issues include ensuring that sensitive information is secured, developing secure communications networks, integrating staff from different organizations, and ensuring that the department has properly skilled staff.

Information Sharing Is Integral to Fulfilling DHS's Mission

With the terrorist attacks of September 2001, the threat of terrorism rose to the top of the country's national security and law enforcement agendas. As stated by the President in his *National Strategy for Homeland Security* in July 2002, our nation's terrorist enemies are constantly seeking new tactics or unexpected ways to carry out their attacks and magnify their effects, such as working to obtain chemical, biological, radiological, and nuclear weapons. In addition, terrorists are gaining expertise in less

[3]Watch lists are automated databases that contain various types of data on individuals, from biographical data—such as a person's name and date of birth—to biometric data such as fingerprints.

traditional means, such as cyber attacks. In response to these growing threats, Congress passed and the President signed the Homeland Security Act of 2002 creating the DHS. The overall mission of this new cabinet-level department includes preventing terrorist attacks in the United States, reducing the vulnerability of the United States to terrorist attacks, and minimizing damage and assisting in recovery from attacks that do occur. To accomplish this mission, the act established specific homeland security responsibilities for the department and directed it to coordinate its efforts and share information within DHS and with other federal agencies, state and local governments, the private sector, and other entities. This information sharing is critical to successfully addressing increasing threats and fulfilling the mission of DHS.

Threats, Incidents, and the Consequences of Potential Attacks Are Increasing

DHS's responsibilities include the protection of our nation's publicly and privately controlled resources essential to the minimal operations of the economy and government against the risks of physical as well as computer-based or cyber attacks. Over the last decade, physical and cyber events, as well as related analyses by various entities, have demonstrated the increasing threat to the United States.

With the coordinated terrorist attacks against the World Trade Center in New York City and the Pentagon in Washington, D.C., on September 11, 2001, the threat of terrorism rose to the top of the country's national security and law enforcement agendas. Even before these catastrophic incidents, the threat of attacks against people, property, and infrastructures had increased concerns about terrorism. The terrorist bombings in 1993 of the World Trade Center in New York City and in 1995 of the Alfred P. Murrah Federal Building in Oklahoma City, which killed 168 people and wounded hundreds of others, prompted increased emphasis on the need to strengthen and coordinate the federal government's ability to effectively combat terrorism domestically. The 1995 Aum Shinrikyo sarin nerve agent attack in the Tokyo subway system also raised new concerns about U.S. preparedness to combat terrorist incidents involving weapons of mass destruction.[4] However, as clearly demonstrated by the September 11, 2001, incidents, a terrorist attack would not have to fit the definition of weapons of mass destruction to result in mass casualties, destruction of critical infrastructures, economic losses, and disruption of daily life nationwide.

[4]A weapon of mass destruction is a chemical, biological, radiological, or nuclear agent or weapon.

U.S. intelligence and law enforcement communities continuously assess both foreign and domestic terrorist threats to the United States. Table 1 summarizes key physical threats to homeland security.

Table 1: Physical Threats to Homeland Security

Threat	Description
Chemical weapons	Chemical weapons are extremely lethal and capable of producing tens of thousands of casualties. They are also relatively easy to manufacture, using basic equipment, trained personnel, and precursor materials that often have legitimate dual uses. As the 1995 Tokyo subway attack revealed, even sophisticated nerve agents are within the reach of terrorist groups.
Biological weapons	Biological weapons, which release large quantities of living, disease-causing microorganisms, have extraordinary lethal potential. Like chemical weapons, biological weapons are relatively easy to manufacture, requiring straightforward technical skills, basic equipment, and a seed stock of pathogenic microorganisms. Biological weapons are especially dangerous because we may not know immediately that we have been attacked, allowing an infectious agent time to spread. Moreover, biological agents can serve as a means of attack against humans as well as livestock and crops, inflicting casualties as well as economic damage.
Radiological weapons	Radiological weapons, or "dirty bombs," combine radioactive material with conventional explosives. The individuals and groups engaged in terrorist activity can cause widespread disruption and fear, particularly in heavily populated areas.
Nuclear weapons	Nuclear weapons have enormous destructive potential. Terrorists who seek to develop a nuclear weapon must overcome two formidable challenges. First, acquiring or refining a sufficient quantity of fissile material is very difficult—though not impossible. Second, manufacturing a workable weapon requires a very high degree of technical capability—though terrorists could feasibly assemble the simplest type of nuclear device. To get around these significant though not insurmountable challenges, terrorists could seek to steal or purchase a nuclear weapon.
Conventional means	Terrorists, both domestic and international, continue to use traditional methods of violence and destruction to inflict harm and spread fear. They have used knives, guns, and bombs to kill the innocent. They have taken hostages and spread propaganda. Given the low expense, ready availability of materials, and relatively high chance for successful execution, terrorists will continue to make use of conventional attacks.

Source: National Strategy for Homeland Security

In addition to these physical threats, terrorists and others with malicious intent, such as transnational criminals and intelligence services, pose a threat to our nation's computer systems. As dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way much of the world communicate and conducts business, this widespread interconnectivity also poses significant risks to the government's and our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. If not properly controlled, the speed and accessibility that

create the enormous benefits of the computer age also allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes.

Government officials are increasingly concerned about cyber attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and are using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data.[5] In addition, the disgruntled organization insider is a significant threat, since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available IT, the likelihood increases that cyber attacks will threaten vital national interests. Table 2 summarizes the key cyber threats to our infrastructure.

[5]*Virus:* a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. *Trojan horse:* a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. *Worm:* an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Logic bomb:* in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. *Sniffer:* synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

Table 2: Cyber Threats to Critical Infrastructure Observed by the FBI

Threat	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Information warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence,[a] can affect the daily lives of Americans across the country.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and "worms" have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, and Code Red.

Source: Federal Bureau of Investigation unless otherwise indicated.

[a]Prepared Statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 2, 2000.

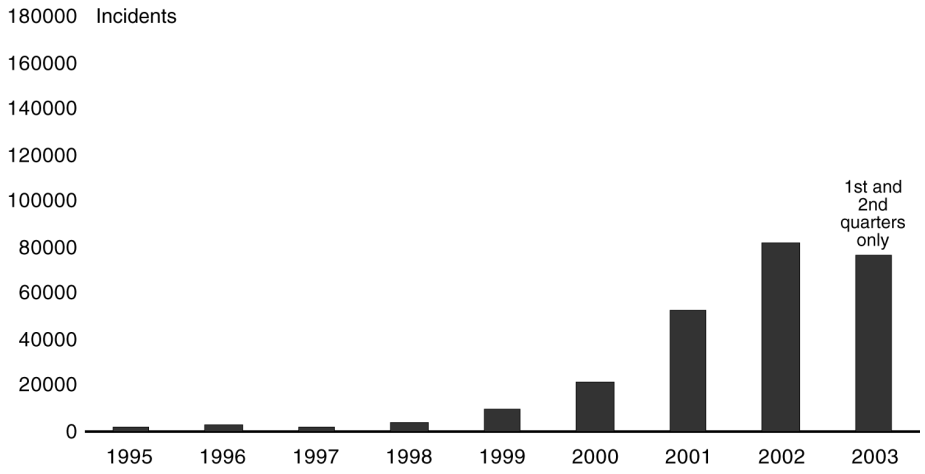
As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A hacker can literally download tools from the Internet and "point and click" to start an attack. Experts also agree that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

Along with these increasing threats, the number of computer security incidents reported to the CERT® Coordination Center[6] has also risen dramatically from just under 10,000 in 1999 to about 82,000 in 2002, and to over 76,000 for the first and second quarters of 2003. And these are only

[6]The CERT® Coordination Center (CERT® CC) is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

the reported attacks. The Director of CERT Centers stated that he estimates that as much as 80 percent of actual security incidents goes unreported, in most cases because (1) the organization was unable to recognize that its systems had been penetrated or there were no indications of penetration or attack or (2) the organization was reluctant to report. Figure 1 shows the number of incidents reported to the CERT Coordination Center from 1995 through the first half of 2003.

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT Coordination Center from 1995 through the First Half of 2003



Source: GAO analysis based on Carnegie-Mellon University's CERT® Coordination Center data.

According to the National Security Agency, foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. Since the terrorist attacks of September 11, 2001, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, in February 2002, the threat to these infrastructures was highlighted by the Special Advisor to the President for Cyberspace Security in a Senate briefing when he stated that although to date none of the traditional terrorists groups, such as al Qaeda, have used the Internet to launch a known assault on the United States' infrastructure, information on water systems was discovered on computers found in al Qaeda camps in Afghanistan.[7] Also, in

[7]"Administrative Oversight: Are We Ready for A Cyber Terror Attack?" Testimony before the Senate Committee on the Judiciary, Subcommittee on Administrative Oversight and the Courts, by Richard A. Clarke, Special Advisor to the President for Cyberspace Security and Chairman of the President's Critical Infrastructure Protection Board (Feb. 13, 2002).

his February 2002 statement for the Senate Select Committee on Intelligence, the director of central intelligence discussed the possibility of cyber warfare attack by terrorists.[8] He stated that the September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them.

Since September 11, 2001, the critical link between cyberspace and physical space has also been increasingly recognized. In his November 2002 congressional testimony, the Director, CERT Centers at Carnegie-Mellon University, noted that supervisory control and data acquisition (SCADA) systems and other forms of networked computer systems have been used for years to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical systems, and that these control systems are increasingly being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions.[9] These computer-controlled and network-connected systems are potential targets for individuals bent on causing massive disruption and physical damage, and the use of commercial, off-the-shelf technologies for these systems without adequate security enhancements can significantly limit available approaches to protection and may increase the number of potential attackers.

Not only is the cyber protection of our critical infrastructures important in and of itself, but a physical attack in conjunction with a cyber attack has also been highlighted as a major concern. In fact, the National Infrastructure Protection Center (NIPC) has stated that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure.[10] As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources

[8] Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 6, 2002.
[9] Testimony of Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Nov. 19, 2002.
[10] National Infrastructure Protection Center, *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption* (Washington, D.C.: July 2002).

needed to manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For example, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack.

Information Sharing is Critical to Meeting DHS's Mission

As our government and our nation has become ever more reliant on interconnected computer systems to support critical operations and infrastructures and as physical and cyber threats and potential attack consequences have increased, the importance of sharing information and coordinating the response to threats among stakeholders has increased. Information sharing and coordination among organizations are central to producing comprehensive and practical approaches and solutions to combating threats. For example, having information on threats and on actual incidents experienced by others can help an organization identify trends, better understand the risk it faces, and determine what preventive measures should be implemented. In addition, comprehensive, timely information on incidents can help federal and nonfederal analysis centers determine the nature of an attack, provide warnings, and advise on how to mitigate an imminent attack. Also, sharing information on terrorists and criminals can help to secure our nation's borders.

The Homeland Security Act of 2002 created DHS with the primary responsibility of preventing terrorist attacks in the United States, reducing the vulnerability of the United States to terrorist attacks, and minimizing damage and assisting in recovery from attacks that do occur. To help DHS accomplish its mission, the act establishes, among other entities, five under secretaries with responsibility over directorates for management, science and technology, information analysis and infrastructure protection**,** border and transportation security**,** and emergency preparedness and response.

As part of DHS's responsibilities, the act includes several provisions specifically related to coordinating and sharing information within the department and among other federal agencies, state and local governments, the private sector, and other entities. It also includes provisions for protecting CIP information shared by the private sector and for sharing different types of information, such as grand jury and intelligence information. Other DHS responsibilities related to information sharing include

- requesting and receiving information from other federal agencies, state and local government agencies, and the private sector relating to threats of terrorism in the United States;
- distributing or, as appropriate, coordinating the distribution of warnings and information with other federal agencies, state and local governments and authorities, and the public;
- creating and fostering communications with the private sector;
- promoting existing public/private partnerships and developing new public/private partnerships to provide for collaboration and mutual support; and
- coordinating and, as appropriate, consolidating the federal government's communications and systems of communications relating to homeland security with state and local governments and authorities, the private sector, other entities, and the public.

Each DHS directorate is responsible for coordinating relevant efforts with other federal, state, and local governments. The act also established the Office for State and Local Government Coordination to, among other things, provide state and local governments with regular information, research, and technical support to assist them in securing the nation. Further, the act included provisions as the "Homeland Security Information Sharing Act" that requires the President to prescribe and implement procedures for facilitating homeland security information sharing and establishes authorities to share different types of information, such as grand jury information; electronic, wire, and oral interception information; and foreign intelligence information. In July 2003, the President assigned these functions to the Secretary of Homeland Security.[11]

The following sections illustrate how DHS will require successful information sharing within the department and between federal agencies, state and local governments, and the private sector to effectively carry out its mission.

[11]The White House, Executive Order 13311— Homeland Security Information Sharing (Washington, D.C.: Jul. 29, 2003).

Information Analysis and Infrastructure Protection Directorate

The Information Analysis and Infrastructure Protection Directorate (IAIP) is responsible for accessing, receiving, and analyzing law enforcement information, intelligence information, and other threat and incident information from respective agencies of federal, state, and local governments and the private sector, and for combining and analyzing such information to identify and assess the nature and scope of terrorist threats. IAIP is also tasked with coordinating with other federal agencies to administer the Homeland Security Advisory System to provide specific warning information along with advice on appropriate protective measures and countermeasures.[12] Further, IAIP is responsible for disseminating, as appropriate, information analyzed by DHS within the department, to other federal agencies, to state and local government agencies, and to private-sector entities.

The Homeland Security Act of 2002 makes DHS and its IAIP directorate also responsible for key CIP functions for the federal government. CIP involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are critical to national security, national economic security, and/or national public health and safety. Information sharing is a key element of these activities. Over 80 percent of our nation's critical infrastructures are controlled by the private sector. As part of its CIP responsibilities, IAIP is responsible for (1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States and (2) recommending measures to protect the key resources and critical infrastructure of the United States in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities.

Federal CIP policy has continued to evolve since the mid-1990s through a variety of working groups, special reports, executive orders, strategies, and organizations. In particular, Presidential Decision Directive 63 (PDD 63) issued in 1998 established CIP as a national goal and described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. To accomplish its goals, PDD 63 established and designated organizations to provide central coordination and support. These included the Critical Infrastructure

[12]The Homeland Security Advisory System uses five levels (Severe, High, Elevated, Guarded, and Low) to inform federal, state, and local government agencies and authorities, the private sector, and the public of the nation's terrorist threat conditions.

Assurance Office (CIAO), an interagency office established to develop a national plan for CIP, and NIPC, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation/response. The Homeland Security Act of 2002 transferred these and certain other CIP entities and their functions (other than the Computer Investigations and Operations Section of NIPC) to DHS's IAIP directorate.

Federal CIP policy, beginning with PDD 63 and reinforced through other strategy documents, including the *National Strategy for Homeland Security* issued in July 2002, called for a range of activities intended to establish a partnership between the public and private sectors to ensure the security of our nation's critical infrastructures. To ensure coverage of critical infrastructure sectors, this policy identified infrastructure sectors that were essential to our national security, national economic security, and/or national public health and safety. For these sectors, which now total 14, federal government leads (sector liaisons) and private-sector leads (sector coordinators) were to work with each other to address problems related to CIP for their sector. In particular, they were to (1) develop and implement vulnerability awareness and education programs and (2) contribute to a sectoral plan by

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing major attacks; and
- developing a plan for alerting, containing, and rebuffing an attack in progress and then, in coordination with the Federal Emergency Management Agency as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

CIP policy also called for sector liaisons to identify and assess economic incentives to encourage the desired sector behavior in CIP. Federal grant programs to assist state and local efforts, legislation to create incentives for the private sector and, in some cases, regulation are mentioned in CIP policy.

Federal CIP policy also encourages the voluntary creation of information sharing and analysis centers (ISACs) to serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC. Their activities could improve the security posture of the individual

sectors, as well as provide an improved level of communication within and across sectors and all levels of government. While PDD 63 encouraged the creation of ISACs, it left the actual design and functions of the ISACs, along with their relationship with NIPC, to be determined by the private sector in consultation with the federal government. PDD 63 did provide suggested activities, which the ISACs could undertake, including

- establishing baseline statistics and patterns on the various infrastructures;
- serving as a clearinghouse for information within and among the various sectors;
- providing a library for historical data for use by the private sector and government; and
- reporting private-sector incidents to NIPC.

As we reported in our April 8, 2003,[13] testimony, table 3 shows the sectors identified in federal CIP policy, the lead agencies for these sectors, and whether or not an ISAC has been established for the sector.

[13]U.S. General Accounting Office, *Information Security Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, GAO-03-564T (Washington, D.C.: Apr. 8, 2003).

Table 3: Lead Agencies and ISAC Status by CIP Sector

Sectors	Designated lead agency	ISAC established
Sectors identified by PDD 63		
Information and telecommunications	Homeland Security*	
Information technology		✓
Telecommunications		✓
Research and education networks		✓
Banking and finance	Treasury	✓
Water	Environmental Protection Agency	✓
Transportation	Homeland Security*	
Aviation		
Surface transportation		✓
Maritime		prospective
Trucking		✓
Emergency services**	Homeland Security*	
Emergency law enforcement		✓
Emergency fire services		✓
Government **	Homeland Security*	
Interstate		✓
Energy	Energy	
Electric power		✓
Oil and gas		✓
Public health	Health and Human Services	
Sectors identified by the *National Strategy for Homeland Security*		
Food		✓
Meat and poultry	Agriculture	
All other food products	Health and Human Services	
Agriculture	Agriculture	
Chemical industry and hazardous materials	Environmental Protection Agency	
Chemicals		✓
Defense industrial base	Defense	
Postal and shipping	Homeland Security	
National monuments and icons	Interior	
Other communities that have established ISACs		
Real estate		✓

*The lead agencies previously designated by PDD 63 were (from top to bottom) the Department of Commerce, Department of Transportation, Department of Justice/Federal Bureau of Investigation, and the Federal Emergency Management Agency.

**PDD 63 identified as critical sectors (1) emergency law enforcement and (2) emergency fire services and continuity of government. In the *National Strategy for Homeland Security*, emergency law enforcement and emergency fire services are both included in an emergency services sector. Also, continuity of government, along with continuity of operations, is listed as a subcomponent under the government sector.

The Interstate ISAC shown in table 3 was established by the National Association of State Chief Information Officers (NASCIO) and is intended to provide a mechanism for informing state officials about DHS threat

warnings, alerts, and other relevant information, and for state officials to report information to DHS. According to a NASCIO official, currently, there are limited resources available to provide suggested ISAC activities. For example, there is not a watch operation, although notifications can be sent out to members at any time and some states have their own watch centers. He also stated that NASCIO's efforts have focused on working with DHS to develop an intergovernmental approach, similar to other federal and state efforts such as law enforcement task forces, where state and federal agencies share resources and responsibilities.

As called for by the *National Strategy for Homeland Security*, on February 14, 2003, the President also released the *National Strategy to Secure Cyberspace* and the complementary *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. These two strategies identify priorities, actions, and responsibilities for the federal government (including lead agencies and DHS) as well as for state and local governments and the private sector. These two strategies also emphasize the importance of developing mechanisms for the public and private sectors to share information about vulnerabilities, incidents, threats, and other security data. For example, the *National Strategy to Secure Cyberspace* calls for the development of a National Cyberspace Security Response System. To be coordinated by DHS, this system is described as a public/private architecture for analyzing and warning, managing incidents of national significance, promoting continuity in government systems and private-sector infrastructures, and increasing information sharing across and between organizations to improve cyberspace security. The system is to include governmental and nongovernmental entities, such as private-sector ISACs. The strategies also encourage the continued establishment of ISACs and efforts to enhance the analytical capabilities of existing ISACs.

As we reported in April 2003, according to a DHS official, the department is continuing to carry out the CIP activities of the functions and organizations transferred to it by the Homeland Security Act of 2002.[14] Further, this official stated that the department is taking actions to enhance those activities as it integrates them within the new department and is continuing previously established efforts to maintain and build relationships with other federal entities, including the FBI and other NIPC partners, and with the private sector.

[14]GAO-03-564T.

To fulfill its mission, the IAIP directorate will need to ensure effective information sharing with other federal entities. For example, information sharing with the recently formed Terrorist Threat Integration Center (TTIC) is a central function of the directorate. TTIC was created to merge and analyze terrorist-related information collected domestically and abroad to enhance coordination, facilitate threat analysis, and enable more comprehensive threat assessments. DHS is providing staff to work at TTIC, and the center is to provide DHS with a comprehensive assessment of threat information that will guide the department's response to any potential attacks.

To help implement its cybersecurity responsibilities, in June 2003, DHS created the National Cyber Security Division within IAIP, and on September 15, 2003, DHS announced the appointment of the first director of the division. According to DHS, this division will identify, analyze, and reduce cyber threats and vulnerabilities; disseminate threat warning information; coordinate incident response; and provide technical assistance in continuity of operations and recovery planning. Building on capabilities transferred to DHS from the CIAO, the NIPC, the Federal Computer Incident Response Center (FedCIRC), and the National Communications System, the division is organized around three units designed to:

- identify risks and help reduce the vulnerabilities to government's cyber assets and coordinate with the private sector to identify and help protect America's critical cyber assets;
- oversee a consolidated Cyber Security Tracking, Analysis, & Response Center, which will detect and respond to Internet events; track potential threats and vulnerabilities to cyberspace; and coordinate cybersecurity and incident response with federal, state, local, private-sector and international partners; and
- create, in coordination with other appropriate agencies, cybersecurity awareness and education programs and partnerships with consumers, businesses, governments, academia, and international communities.

Also, on September 15, 2003, DHS announced the creation of the U.S. Computer Emergency Response Team (US–CERT)—a partnership between the National Cyber Security Division and CERT/CC. According to DHS, it will

- improve warning and response time to security incidents by fostering the development of detection tools and using common commercial incident and vulnerability reporting protocols—with the goal to reduce the

response time to a security event to an average of 30 minutes by the end of 2004;

- increase the flow of critical security information throughout the Internet community;
- provide a coordination center that, for the first time, links public and private response capabilities to facilitate communication across all infrastructure sectors;
- collaborate with the private sector to develop and implement new tools and methods for detecting and responding to vulnerabilities; and
- work with infrastructure owners and operators and technology experts to foster the development of improved security technologies and methods to increase cybersecurity at all levels across the nation.

In its announcement, DHS also stated that the US–CERT is expected to grow to include other partnerships with private-sector security vendors and other domestic and international CERT organizations. These groups will work together to coordinate national and international efforts to prevent, protect, and respond to the effects of cyber attacks across the Internet.

The Directorate of Border and Transportation Security

According to the act, the Border and Transportation Security Directorate (BTS) is responsible for, among other things, (1) preventing the entry of terrorists and the instruments of terrorism into the United States; (2) securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems, including managing and coordinating those functions transferred to the department; (3) carrying out immigration enforcement functions; (4) establishing and administering rules for granting visas, and (5) administering customs laws. A number of federal entities are under its responsibility, such as the Transportation Security Administration, U.S. Customs Service, the border security functions of the Immigration and Naturalization Service (INS), Animal and Plant Health Inspection Service, and the Federal Law Enforcement Training Center.

To successfully protect the borders and transportation systems of the United States, BTS faces the challenge of sharing information across the various organizations under its responsibility. According to the *National Strategy for Homeland Security*, to successfully prevent the entry of

contraband, unauthorized aliens, and potential terrorists, DHS will have to increase the level of information available on inbound goods and passengers to the border management component agencies under the BTS. For example, the strategy discusses the need to increase the security of international shipping containers—noting that 50 percent of the value of U.S. imports arrives via 16 million containers. To increase security, U.S. inspectors will need shared information so that they can identify high-risk containers. In addition, protecting our borders from the entry of unauthorized aliens and potential terrorists will require the sharing of information between various law enforcement and immigration services. For example, we recently reported on the use of watch lists as important tools to help secure our nation's borders.[15] These lists provide decision makers with information about individuals who are known or suspected terrorists and criminals so that these individuals can be prevented from entering the country, apprehended while in the country, or apprehended as they attempt to exit the country.

The Emergency Preparedness and Response Directorate

According to the act, the Emergency Preparedness and Response Directorate (EPR) ensures that the nation is prepared for, and able to recover from, terrorist attacks, major disasters, and other emergencies. In addition, EPR is responsible for building a comprehensive national incident management system with federal, state, and local governments and authorities to respond to such attacks and disasters. This project will require developing an extensive program of information sharing among federal, state, and local governments. Further, EPR is to develop comprehensive programs for developing interoperable communications technology and helping to ensure that emergency response providers acquire such technology. Among the functions transferred to EPR are the Federal Emergency Management Agency, the Integrated Hazard Information System of the National Oceanic and Atmospheric Administration, and the Metropolitan Medical Response System.

Information sharing is important to emergency responders to prepare for and respond to terrorist attacks and other emergencies. For example, if a biological attack were to occur, it would be important for health officials to quickly and effectively exchange information with relevant experts directly responding to the event in order to respond appropriately. To

[15]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).

support this type of exchange, the Centers for Disease Control and Prevention (CDC) created the Epidemic Information Exchange (*Epi-X*), a secure, Web-based communications network that serves as an information exchange between CDC, state and local health departments, poison control centers, and other public health professionals. According to CDC, *Epi-X's* primary goals include informing health officials about important public health events, helping them respond to public health emergencies, and encouraging professional growth and the exchange of information**.** CDC has also created an emergency operations center to respond to public health emergencies and to allow for immediate secure communication between CDC, the Department of Health and Human Services, federal intelligence and emergency response officials, DHS, and state and local public health officials.

Information Sharing Challenges

We have made numerous recommendations over the last several years related to information sharing functions that have been transferred to DHS. One significant area of our work concerns the federal government's CIP efforts, which is focused on sharing information on incidents, threats, and vulnerabilities and providing warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments and the private sector. Although improvements have been made in protecting our nation's critical infrastructures and continuing efforts are in progress, further efforts are needed to address the following critical CIP challenges that we have identified:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing, which clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;
- developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector;
- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector; and

- providing appropriate incentives for nonfederal entities to increase information sharing with the federal government.

In addition, we recently identified challenges in consolidating and standardizing watch list structures and policies, which are essential to effectively sharing information on suspected criminals and terrorists.

A Complete and Coordinated National CIP Plan Needs to Be Developed

An underlying issue in the implementation of CIP is that no national plan to facilitate information sharing yet exists that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets time frames for achieving objectives, and establishes performance measures. Such a clearly defined plan is essential for defining the relationships among all CIP organizations to ensure that the approach is comprehensive and well coordinated. Since 1998, we have reported on the need for such a plan and made numerous related recommendations.

In September 1998, we reported that developing a governmentwide strategy that clearly defined and coordinated the roles of federal entities was important to ensure governmentwide cooperation and support for PDD 63.[16] At that time, we recommended that the Office of Management and Budget (OMB) and the Assistant to the President for National Security Affairs ensure such coordination.

In January 2000, the President issued *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. The plan proposed achieving the twin goals of making the U.S. government a model of information security and developing a public/private partnership to defend our national infrastructures. However, this plan focused largely on federal cyber CIP efforts, saying little about the private-sector role.

In September 2001, we reported that agency questions had surfaced regarding specific roles and responsibilities of entities involved in cyber CIP and the timeframes within which CIP objectives were to be met, as

[16]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998).

well as guidelines for measuring progress.[17] Accordingly, we made several recommendations to supplement those we had made in the past. Specifically, we recommended that the Assistant to the President for National Security Affairs ensure that the federal government's strategy to address computer-based threats define

- specific roles and responsibilities of organizations involved in CIP and related information security activities;
- interim objectives and milestones for achieving CIP goals and a specific action plan for achieving these objectives, including implementing vulnerability assessments and related remedial plans; and
- performance measures for which entities can be held accountable.

In July 2002, we issued a report identifying at least 50 organizations that were involved in national or multinational cyber CIP efforts, including 5 advisory committees; 6 Executive Office of the President organizations; 38 executive branch organizations associated with departments, agencies, or intelligence organizations; and 3 other organizations.[18] Although our review did not cover organizations with national physical CIP responsibilities, the large number of organizations that we did identify as involved in CIP efforts presents a need to clarify how these entities coordinate their activities with each other. Our report also stated that PDD 63 did not specifically address other possible critical sectors and their respective federal agency counterparts. Accordingly, we recommended that the federal government's strategy also

- include all relevant sectors and define the key federal agencies' roles and responsibilities associated with each of these sectors, and
- define the relationships among the key CIP organizations.

In July 2002, the *National Strategy for Homeland Security* called for interim cyber and physical infrastructure protection plans that DHS would use to build a comprehensive national infrastructure plan. Implementing a well-developed plan is critical to effective coordination in times of crises. According to the strategy, the national plan is to provide a methodology for identifying and prioritizing critical assets, systems, and functions, and

[17]U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, D.C.: Sept. 20, 2001).
[18]GAO-02-474.

for sharing protection responsibility with state and local governments and the private sector. The plan is also to establish standards and benchmarks for infrastructure protection and provide a means to measure performance. The plan is expected to inform DHS on budgeting and planning for CIP activities and how to use policy instruments to coordinate between government and private entities to improve the security of our national infrastructures to appropriate levels. The strategy also states that DHS is to unify the currently divided responsibilities for cyber and physical security. According to the department's November 2002 reorganization plan, the Assistant Secretary for Infrastructure Protection is responsible for developing a comprehensive national infrastructure plan.

As discussed previously, in February 2003, the President issued the interim strategies—*The National Strategy to Secure Cyberspace* and *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (hereafter referred to in this testimony as the cyberspace security strategy and the physical protection strategy). These strategies identify priorities, actions, and responsibilities for the federal government, including federal lead departments and agencies and the DHS, as well as for state and local governments and the private sector. Both define strategic objectives for protecting our nation's critical assets. The physical protection strategy discusses the goals and objectives for protecting our nation's critical infrastructure and key assets from physical attack. The cyberspace security strategy provides a framework for organizing and prioritizing the individual and concerted responsibilities of all levels of government to secure cyberspace.

According to the physical protection strategy, across government, there are inconsistent methodologies to prioritize efforts to enhance critical infrastructure protection. This problem is compounded with ineffective communication among the federal, state, and local governments that has resulted in untimely, disparate, and at times conflicting communication between those who need it most. DHS has been given a primary role in providing cross-sector coordination to improve communication and planning efforts and serves as the single point of coordination for state and local governments on homeland security issues. To fulfill its role as the cross-sector coordinator, DHS will partner with state and local governments and the private sector to institute processes that are transparent, comprehensive, and results-oriented. This effort will include creating mechanisms for collaborative national planning efforts between the private and public sectors and for consolidating the individual sector plans into a comprehensive plan that will define their respective roles, responsibilities, and expectations.

The cyberspace security strategy is the counterpart to the physical protection strategy and provides the framework for organizing and prioritizing the individual and concerted responsibilities of all levels of government to secure cyberspace. DHS serves as the focal point for managing cybersecurity incidents that could affect the federal government or the national information infrastructure and, thus, plays a central role in executing the initiatives assigned in this strategy. While the cyberspace security strategy mentions the responsibility of DHS in creating a comprehensive national plan for securing resources and key infrastructures, much of the strategy's emphasis remains on coordinating and integrating various plans with the private sector.

Neither strategy (1) clearly indicates how the physical and cyber efforts will be coordinated; (2) defines the roles, responsibilities, and relationships among the key CIP organizations, including state and local governments and the private sector; (3) indicates time frames or milestones for their overall implementation or for accomplishing specific actions or initiatives; nor (4) establishes performance measures for which entities can be held responsible. Until a comprehensive and coordinated plan is completed that unifies the responsibilities for cyber and physical infrastructures; identifies roles, responsibilities, and relationships for all CIP efforts; establishes time frames or milestones for implementation; and establishes performance measures, our nation risks not having a consistent and appropriate information sharing framework to deal with growing threats to its critical infrastructure.

Better Information Sharing on Threats and Vulnerabilities Must Be Implemented

Information sharing is a key element in developing comprehensive and practical approaches to defending against potential cyber and other attacks, which could threaten the national welfare. Information on threats, vulnerabilities, and incidents experienced by others can help identify trends, better understand the risks faced, and determine what preventive measures should be implemented. However, as we have reported in recent years, establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult. In addition, the private sector has expressed concerns about sharing information with the government and the difficulty of obtaining security clearances. Both the Congress and the administration have taken steps to address information sharing issues in law and recent policy guidance, but their effectiveness will largely depend on how DHS implements its information sharing responsibilities.

A number of activities have been undertaken to build information-sharing relationships between the federal government and the private sector, such as InfraGard, the Partnership for Critical Infrastructure Security, efforts by the CIAO, and efforts by lead agencies to establish ISACs. For example, the InfraGard Program, which provides the FBI and NIPC with a means of securely sharing information with individual companies, has expanded substantially. InfraGard membership has increased from 277 in October 2000 to almost 9,400 in September 2003. Members include representatives from private industry, other government agencies, state and local law enforcement, and the academic community.

As stated above, PDD 63 encouraged the voluntary creation of ISACs to serve as the mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information between the private sector and the federal government through NIPC. In April 2001, we reported that NIPC and other government entities had not developed fully productive information-sharing relationships but that NIPC had undertaken a range of initiatives to foster information-sharing relationships with ISACs, as well as with government and international entities. We recommended that NIPC formalize relationships with ISACs and develop a plan to foster a two-way exchange of information between them.

In response to our recommendations, NIPC officials told us in July 2002 that an ISAC development and support unit had been created, whose mission was to enhance private-sector cooperation and trust so that it would result in a two-way sharing of information. As shown previously in table 3, as of April 2003, DHS reported that there are 16 current ISACs, including ISACs established for sectors not identified as critical infrastructure sectors. DHS officials also stated that they have formal agreements with most of the current ISACs.

In spite of progress made in establishing ISACs, additional efforts are needed. All sectors do not have a fully established ISAC, and even for those sectors that do, our recent work showed that participation may be mixed, and the amount of information being shared between the federal government and private-sector organizations also varies. Specifically, as we reported in February 2003, the five ISACs we recently reviewed showed different levels of progress in implementing the PDD 63 suggested activities.[19] For example, four of the five reported that efforts were still in progress to establish baseline statistics, which includes developing a

[19]U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, D.C.: Feb. 28, 2003).

database on the normal levels of computer security incidents that would be used for analysis purposes. Also, while all five reported that they served as the clearinghouse of information (such as incident reports and warnings received from members) for their own sectors, only three of the five reported that they are also coordinating with other sectors. Only one of the five ISACs reported that it provides a library of incidents and historical data that was available to both the private sector and the federal government, and although three additional ISACs do maintain a library, it was available only to the private sector. Table 4 summarizes the reported status of the five ISACs in performing these and other activities suggested by PDD 63.

Table 4: ISACs' Progress in Performing Activities Suggested by PDD 63

	ISAC				
Activity	**Telecommunications**	**Electricity**	**Information Technology**	**Energy**	**Water**
Establish baseline statistics	In progress	In progress	Yes	In progress	In progress
Serve as clearinghouse within and among sectors	Yes	Yes	Yes	Only within own sector	Only within own sector
Provide library to private sector and government	In progress	Yes	Available only to private sector	Available only to private sector	Available only to private sector
Report incidents to NIPC	Yes	Yes	Yes	No	Yes

Source: ISACs.

As also noted in our February 2003 report, some in the private sector expressed concerns about voluntarily sharing information with the government. Specifically, concerns were raised that industry could potentially face antitrust violations for sharing information with other industry partners, have their information subject to the Freedom of Information Act (FOIA), or face potential liability concerns for information shared in good faith. For example, the IT, energy, and the water ISACs reported that they did not share their libraries with the federal government because of concerns that information could be released under FOIA. And, officials of the energy ISAC stated that they have not reported incidents to NIPC because of FOIA and antitrust concerns.

The recently established ISAC Council may help to address some of these concerns. According to its chairman, the mission of the ISAC Council is to advance the physical and cybersecurity of the critical infrastructures of North America by establishing and maintaining a framework for interaction between and among the ISACs. Activities of the council include establishing and maintaining a policy for inter-ISAC coordination, a dialog with governmental agencies that deal with ISACs, and a practical data and information sharing protocol (what to share and how to share). In

addition, the council will develop analytical methods to assist the ISACs in supporting their own sectors and other sectors with which there are interdependencies and establish a policy to deal with matters of liability and anti-trust. The chairman also reported that the council held an initial meeting with DHS and the White House in June 2003 to, among other things, understand mutual DHS and ISAC expectations.

There will be continuing debate as to whether adequate protection is being provided to the private sector as these entities are encouraged to disclose and exchange information on both physical and cybersecurity problems and solutions that are essential to protecting our nation's critical infrastructures. The *National Strategy for Homeland Security* includes "enabling critical infrastructure information sharing" in its 12 major legislative initiatives. It states that the nation must meet this need by narrowly limiting public disclosure of information relevant to protecting our physical and cyber critical infrastructures in order to facilitate the voluntary submission of information. It further states that the Attorney General will convene a panel to propose any legal changes necessary to enable sharing of essential homeland security related information between the federal government and the private sector.

Actions have already been taken by the Congress and the administration to strengthen information sharing. For example, the USA PATRIOT Act promotes information sharing among federal agencies, and numerous terrorism task forces have been established to coordinate investigations and improve communications among federal and local law enforcement.[20] Moreover, the Homeland Security Act of 2002 includes provisions that restrict federal, state, and local government use and disclosure of critical infrastructure information that has been voluntarily submitted to DHS. These restrictions include exemption from disclosure under FOIA, a general limitation on use to CIP purposes, and limitations on use in civil actions and by state or local governments. The act also provides penalties for any federal employee who improperly discloses any protected critical infrastructure information. In April 2003, DHS issued for comment its proposed rules for how critical infrastructure information volunteered by the public will be protected. At this time, it is too early to tell what impact the act will have on the willingness of the private sector to share critical infrastructure information.

[20]The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Public Law No. 107-56, October 26, 2001.

Information sharing among federal, state and local governments also needs to be improved. In August 2003 we reported the results of our survey of federal, state, and city government officials' perceptions of the effectiveness of the current information-sharing process.[21] Performed primarily before DHS began its operations, our survey identified some notable information-sharing initiatives, but also highlighted coordination issues and other concerns that many of the surveyed entities had with the overall information-sharing process. For example, the FBI reported it had significantly increased the number of its Joint Terrorism Task Forces and, according to our survey, 34 of 40 states and 160 of 228 cities stated that they participated in information-sharing centers. However, although such initiatives may increase the sharing of information to fight terrorism, none of the three levels of government perceived the current information-sharing process as effective, particularly when sharing information with federal agencies. Respondents reported that information on threats, methods, and techniques of terrorists was not routinely shared; and the information that was shared was not perceived as timely, accurate, or relevant. Further, 30 of 40 states and 212 of 228 cities responded that they were not given the opportunity to participate in national policy making on information sharing. Federal agencies in our survey also identified several barriers to sharing threat information with state and city governments, including 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.

The private sector has also expressed its concerns about the value of information being provided by the government. For example, in July 2002 the President for the Partnership for Critical Infrastructure Security stated in congressional testimony that information sharing between the government and private sector needs work, specifically, in the quality and timeliness of cybersecurity information coming from the government.[22] In March 2003 we also reported that the officials from the chemical industry noted that they need better threat information from law enforcement agencies, as well as better coordination among agencies providing threat information.[23] They stated that chemical companies do not receive enough specific threat information and that it frequently comes from multiple

[21]U.S. General Accounting Office, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760 (Washington, D.C.: Aug. 27, 2003).
[22]Testimony of Kenneth C. Watson, President, Partnership for Critical Infrastructure Security, before the Subcommittee on Oversight and Investigation of the Energy and Commerce Committee, U.S. House of Representatives, July 9, 2002.
[23]U. S. General Accounting Office, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-439 (Washington D.C.: Mar. 14, 2003).

government agencies. Similarly, in developing a vulnerability assessment methodology to assess the security of chemical facilities against terrorist and criminal attacks, the Department of Justice observed that chemical facilities need more specific information about potential threats in order to design their security systems and protocols. Chemical industry officials also noted that efforts to share threat information among industry and federal agencies will be effective only if government agencies provide specific and accurate threat information. Threat information also forms the foundation for some of the tools available to industry for assessing facility vulnerabilities. The Justice vulnerability assessment methodology requires threat information as the foundation for hypothesizing about threat scenarios, which form the basis for determining site vulnerabilities.

The Homeland Security Act, the *National Strategy for Homeland Security*, the *National Strategy to Secure Cyberspace*, and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* all acknowledge the importance of information sharing and identify multiple responsibilities for DHS to share information on threats and vulnerabilities. In particular:

- The Homeland Security Act authorizes the IAIP Under Secretary to have access to all information in the federal government that concerns infrastructure or other vulnerabilities of the United States to terrorism and to use this information to fulfill its responsibilities to provide appropriate analysis and warnings related to threats to and vulnerabilities of critical information systems, crisis management support in response to threats or attacks on critical information systems, and technical assistance upon request to private-sector and government entities to respond to major failures of critical information systems.
- The *National Strategy for Homeland Security* specifies the need for DHS to work with state and local governments to achieve "seamless communication" among all responders. This responsibility includes developing a national emergency communication plan to establish policies and procedures to improve the exchange of information**.** Ensuring improved communications also involves developing systems that help prevent attacks and minimize damage. Such systems, which would be accessed and used by all levels of government, would detect hostile intents and help locate individual terrorists as well as monitor and detect outbreaks**.**
- The cyberspace security strategy encourages DHS to work with the National Infrastructure Advisory Council and the private sector to develop an optimal approach and mechanism to disclose vulnerabilities in order to

expedite the development of solutions without creating opportunities for exploitation by hackers. DHS is also expected to raise awareness about removing obstacles to sharing information concerning cybersecurity and infrastructure vulnerabilities between the public and private sectors and is encouraged to work closely with ISACs to ensure that they receive timely and actionable threat and vulnerability data and to coordinate voluntary contingency planning efforts.

- The physical protection strategy describes DHS's need to collaborate with the intelligence community and the Department of Justice to develop comprehensive threat collection, assessment, and dissemination processes that are distributed to the appropriate entity in a timely manner. It also enumerates several initiatives directed to DHS to accomplish to create a more effective information-sharing environment among the key stakeholders, including establishing requirements for sharing information; supporting state and local participation with ISACs to more effectively communicate threat and vulnerability information; protecting secure and proprietary information deemed sensitive by the private sector; implementing processes for collecting, analyzing, and disseminating threat data to integrate information from all sources; and developing interoperable systems to share sensitive information among government entities to facilitate meaningful information exchange.
- The *National Strategy for Homeland Security* also describes DHS's need to engage its partners around the world in cooperative efforts to improve security. It states that DHS will increase information sharing between the international law enforcement, intelligence, and military communities.

Analysis and Warning Capabilities Need to Be Improved

Analysis and warning capabilities should be developed to detect precursors to attacks on the nation so that advanced warnings can be issued and protective measures implemented. Since the 1990s, the national security community and the Congress have identified the need to establish analysis and warning capabilities to protect against strategic computer attacks against the nation's critical computer-dependent infrastructures. Such capabilities need to address both cyber and physical threats and involve (1) gathering and analyzing information for the purpose of detecting and reporting otherwise potentially damaging actions or intentions and (2) implementing a process for warning policymakers and allowing them time to determine the magnitude of the related risks.

In April 2001,[24] we reported on NIPC's progress and impediments in developing analysis and warning capabilities for computer-based attacks, which included the following:[25]

- Lack of a generally accepted methodology for analyzing strategic cyber-based threats. For example, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.
- Lack of industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. In September 2001, we reported that although outreach efforts had raised awareness and improved information sharing, substantive, comprehensive analysis of infrastructure sector interdependencies and vulnerabilities had been limited.

Another challenge confronting the analysis and warning capabilities of our nation is that, historically, our national CIP attention and efforts have been focused on cyber threats. As we also reported in April 2001, although PDD 63 covers both physical and cyber threats, federal efforts to meet the directive's requirements have pertained primarily to cyber threats since this is an area that the leaders of the administration's CIP strategy view as needing attention. However, the terrorist attacks of September 11, 2001, have increased the emphasis of physical threats. In addition, in July 2002, NIPC reported that the potential for concurrent cyber and physical ("swarming") attacks is an emerging threat to the U.S. critical infrastructure. Further, in July 2002, the director of NIPC also told us that NIPC had begun to develop some capabilities for identifying physical CIP threats. For example, NIPC had developed thresholds with several ISACs for reporting physical incidents and, since January 2002, has issued several information bulletins concerning physical CIP threats. However, NIPC's director acknowledged that fully developing this capability would be a significant challenge. The physical protection strategy states that DHS will maintain a comprehensive, up-to-date assessment of vulnerabilities across

[24] GAO-01-323.
[25] Pursuant to the Homeland Security Act of 2002, the functions of NIPC (except for computer investigations and operations) were transferred over to DHS from the FBI.

sectors and improve processes for domestic threat data collection, analysis, and dissemination to state and local governments and private industry.

The administration and the Congress continue to emphasize the need for these analysis and warning capabilities. The *National Strategy for Homeland Security* identified intelligence and warning as one of six critical mission areas and called for major initiatives to improve our nation's analysis and warning capabilities. The strategy also stated that no government entity was then responsible for analyzing terrorist threats to the homeland, mapping these threats to our vulnerabilities, and taking protective action. The Homeland Security Act gives such responsibility to the new DHS. For example, the IAIP Under Secretary is responsible for administering the Homeland Security Advisory System, and is to coordinate with other federal agencies to provide specific warning information and advice to state and local agencies, the private sector, the public, and other entities about appropriate protective measures and countermeasures to homeland security threats.

An important aspect of improving our nation's analysis and warning capabilities is having comprehensive vulnerability assessments. The *National Strategy for Homeland Security* also states that comprehensive vulnerability assessments of all of our nation's critical infrastructures are important from a planning perspective in that they enable authorities to evaluate the potential effects of an attack on a given sector and then invest accordingly to protect it. The strategy states that the U.S. government does not perform vulnerability assessments of the nation's entire critical infrastructure. The Homeland Security Act of 2002 states that the DHS's IAIP Under Secretary is to carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructures of the United States.

Another critical issue in developing effective analysis and warning capabilities is to ensure that appropriate intelligence and other threat information, both cyber and physical, is received from the intelligence and law enforcement communities. For example, there has been considerable public debate regarding the quality and timeliness of intelligence data shared between and among relevant intelligence, law enforcement, and other agencies. Also, as the transfer of NIPC to DHS organizationally separated it from the FBI's law enforcement activities (including the Counterterrorism Division and NIPC field agents), it will be critical to establish mechanisms for continued communication to occur. Further, it will be important that the relationships between the law enforcement and intelligence communities and the new DHS are effective and that

appropriate information is exchanged on a timely basis. The act gives DHS broad statutory authority to access intelligence information, as well as other information relevant to the terrorist threat and to turn this information into useful warnings. For example, DHS is to be a key participant in the multiagency TTIC[26] that began operations on May 1, 2003. According to a White House fact sheet, DHS's IAIP is to receive and analyze terrorism-related information from the TTIC.[27] Although the purpose of TTIC and the authorities and responsibilities of the FBI and Central Intelligence Agency (CIA) counterterrorism organizations remain distinct, in July 2003, the TTIC Director reported that initiatives are under way to facilitate efforts within the intelligence community to ensure that DHS has access to all information required to execute its mission. He also reported other progress, such as updates to a TTIC-sponsored Web site that provides terrorism-related information. For example, the Web site is to increasingly include products tailored to the needs of state and local officials, as well as private industry.

In addition, according to NIPC's director, as of July 2002, a significant challenge in developing a robust analysis and warning function is the development of the technology and human capital capacities to collect and analyze substantial amounts of information. Similarly, the Director of the FBI testified in June 2002 that implementing a more proactive approach to preventing terrorist acts and denying terrorist groups the ability to operate and raise funds require a centralized and robust analytical capacity that did not then exist in the FBI's Counterterrorism Division.[28] He also stated that processing and exploiting information gathered domestically and abroad during the course of investigations require an enhanced analytical and data mining capacity that was not then available. According to DHS's reorganization plans, the IAIP Under Secretary and the chief information officer (CIO) of the department are to fulfill their responsibilities as laid out by the act to establish and uses a secure communications and IT infrastructure. This infrastructure is to include data-mining and other analytical tools in order to access, receive, analyze, and disseminate data and information.

[26]The center was formed from elements of the Department of Homeland Security, the FBI's Counterterrorism Division, the Director of Central Intelligence's Counterterrorist Center, and the Department of Defense.
[27]The White House, *Fact Sheet: Strengthening Intelligence to Better Protect America* (Washington, D.C.: Jan. 28, 2003).
[28]Testimony of Robert S. Mueller, III, Director Federal Bureau of Investigation, before the Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, Committee on Appropriations, U.S. House of Representatives, June 21, 2002.

Additional Incentives Are Needed to Encourage Increased Information Sharing Efforts

PDD 63 stated that sector liaisons should identify and assess economic incentives to encourage sector information sharing and other desired behavior. Consistent with the original intent of PDD 63, the *National Strategy for Homeland Security* states that, in many cases, sufficient incentives exist in the private market for addressing the problems of CIP. However, the strategy also discusses the need to use all available policy tools to protect the health, safety, or well-being of the American people. It mentions federal grant programs to assist state and local efforts, legislation to create incentives for the private sector, and, in some cases, regulation. The physical protection strategy reiterates that additional regulatory directives and mandates should only be necessary in instances where the market forces are insufficient to prompt the necessary investments to protect critical infrastructures and key assets. The cyberspace security strategy also states that the market is to provide the major impetus to improve cybersecurity and that regulation will not become a primary means of securing cyberspace.

Last year, the Comptroller General testified on the need for strong partnerships with those outside the federal government and that the new department would need to design and manage tools of public policy to engage and work constructively with third parties.[29] We have also previously testified on the choice and design of public policy tools that are available to governments.[30] These public policy tools include grants, regulations, tax incentives, and regional coordination and partnerships to motivate and mandate other levels of government or the private sector to address security concerns. Some of these tools are already being used, such as in the water and chemical sectors.

Without appropriate consideration of public policy tools, private-sector participation in sector-related information sharing and other CIP efforts may not reach its full potential. For example, we reported in January 2003[31] on the efforts of the financial services sector to address cyber threats, including industry efforts to share information and to better foster and facilitate sectorwide efforts. We also reported on the efforts of federal entities and regulators to partner with the financial services industry to

[29]U.S. General Accounting Office, Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will Be Pivotal to Success, GAO-01-886T (Washington, D.C.: June 25, 2002).
[30]U.S. General Accounting Office, *Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy*, GAO-02-549T (Washington, D.C.: Mar. 28, 2002).
[31]U.S. General Accounting Office, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, GAO-03-173 (Washington, DC,: Jan. 30, 2003).

protect critical infrastructures and to address information security. We found that although federal entities had a number of efforts ongoing, Treasury, in its role as sector liaison, had not undertaken a comprehensive assessment of the potential public policy tools to encourage the financial services sector in implementing information sharing and other CIP-related efforts. Because of the importance of considering public policy tools to encourage private-sector participation, we recommended that Treasury assess the need for public policy tools to assist the industry in meeting the sector's goals. In addition, in February 2003, we reported on the mixed progress five ISACs had made in accomplishing the activities suggested by PDD 63. We recommended that the responsible lead agencies assess the need for public policy tools to encourage increased private-sector CIP activities and greater sharing of intelligence and incident information between the sectors and the federal government.

The President's fiscal year 2004 budget request for the new DHS includes $829 million for information analysis and infrastructure protection, a significant increase from the estimated $177 million for fiscal year 2003. In particular, the requested funding for protection includes about $500 million to identify key critical infrastructure vulnerabilities and support the necessary steps to ensure that security is improved at these sites. Although the funding also includes almost $300 million for warning advisories, threat assessments, a communications system, and outreach efforts to state and local governments and the private sector, additional incentives may still be needed to encourage nonfederal entities to increase their CIP efforts.

Consolidating and Standardizing Watch List Structures and Policies

We recently reported on the terrorist and criminal watch list systems maintained by different federal agencies.[32] These watch lists are important information-sharing tools for securing our nation's borders against terrorists. Simply stated, watch lists can be viewed as automated databases that are supported by certain analytical capabilities. These lists contain various types of data, from biographical data—such as a person's name and date of birth—to biometric data such as fingerprints. Nine federal agencies,[33] which before the establishment of DHS spanned five

[32]GAO-03-322.

[33]The nine agencies are the State Department's Bureau of Intelligence and Research and Bureau of Consular Affairs; the Justice Department's Federal Bureau of Investigation, Immigration and Naturalization Service, U.S. Marshals Service, and the U.S. National Central Bureau for Interpol; the Department of Defense's Air Force Office of Special Investigations; the Transportation Department's

different cabinet-level departments,[34] currently maintain 12 terrorist and criminal watch lists. These lists are also used by at least 50 federal, state, and local agencies.

According to the *National Strategy for Homeland Security*, in the aftermath of the September 11th attacks, it became clear that vital watch list information stored in numerous and disparate databases was not available to the right people at the right time. In particular, federal agencies that maintained information about terrorists and other criminals had not consistently shared it. The strategy attributed these information-sharing limitations to legal, cultural, and technical barriers that resulted in the watch lists being developed in different ways, for different purposes, and in isolation from one another. To address these limitations, the strategy provides for developing a consolidated watch list that would bring together the information on known or suspected terrorists contained in federal agencies' respective lists.

As we reported, we found that the watch lists include overlapping but not identical sets of data, and that different policies and procedures govern whether and how these data are shared with others. As a general rule, we found that this information sharing is more likely to occur among federal agencies than between federal agencies and either state and local governments agencies or private entities. Among other things, we also found that the extent to which such information sharing is accomplished electronically is constrained by fundamental differences in the watch lists' systems architecture. Also, differences in agencies' cultures have been and remain one of the principal impediments to integrating and sharing information from watch lists and other information. We recommended that the Secretary of DHS, in collaboration with the heads of other departments and agencies that have or use watch lists, lead an effort to consolidate and standardize the federal government's watch list structures and policies to promote better integration and information sharing. DHS generally agreed with our findings and recommendations.

Transportation Security Administration; and the Treasury Department's U.S. Customs Service. Of these, the Immigration and Naturalization Service, the Transportation Security Administration, and the U.S. Customs Service have been incorporated into the new DHS.

[34]These departments are the Departments of State, Treasury, Transportation, Justice, and Defense.

Effective Systems and Processes Need to Be Established to Facilitate Information Sharing

The success of homeland security relies on establishing effective systems and processes to facilitate information sharing among government entities and the private sector. In May 2003, the CIO of DHS stated that a key goal to protecting our nation is to put in place mechanisms that provide the right information to the right people in a timely manner. He further stated that with the use of IT, homeland security officials throughout the United States will have a more complete awareness of threats and vulnerabilities, as well as knowledge of the personnel and resources available to conquer those threats. We have identified critical success factors to information sharing that DHS should consider. Also, in addition to the need to develop technological solutions, key management issues that DHS must overcome to achieve success include

- integrating existing IT resources of 22 different agencies,
- making new IT investments,
- ensuring that sensitive information is secured,
- developing secure communications networks,
- developing a performance focus,
- integrating staff from different organizations and ensuring that the department has properly skilled staff, and
- ensuring effective oversight.

Addressing these issues will be critical to establishing the effective systems and processes required to facilitate information sharing within the new department.

Success Factors for Sharing Information

In October 2001, we reported on information sharing practices of organizations that successfully share sensitive or time-critical information.[35] We found that these practices include:

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

Among the organizations we studied, we found some very good models to learn from and build on. For example, CERT/CC is charged with establishing a capability to quickly and effectively coordinate communication between experts in order to limit damage, responding to incidents, and building awareness of security issues across the Internet community. In this role, CERT/CC receives Internet security-related information from system and network administrators, technology managers, and policymakers and provides them with this information along with guidance and coordination to major security events. Further, the Agora is a Seattle-based regional network that at the time of our study had over 600 professionals representing various fields, including information systems security; law enforcement; local, state, and federal governments; engineering; IT; academics; and other specialties. Members work to establish confidential ways for organizations to share sensitive information about common problems and best practices for dealing with security threats. They develop and share knowledge about how to protect electronic infrastructures, and they prompt more research specific to electronic information systems security.

In addition, we have previously reported on several other key considerations in establishing effective information sharing, including:

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

- identifying and agreeing on the types of information to be collected and shared between parties,
- developing standard terms and reporting thresholds,
- balancing varying interests and expectations, and
- determining the right format and standards for collecting data so that disparate agencies can aggregate and integrate data sets.

Some efforts have already taken place in these areas. For example, NIPC obtained information-sharing agreements with most ISACs, which included specific reporting thresholds for physical and cyber incidents. Also, incident reporting thresholds have been publicly issued. It will be important for DHS to incorporate these considerations into its information-sharing efforts.

Developing Technological Solutions

Developing and implementing appropriate technological solutions can improve the effectiveness and efficiency of information sharing. We have previously reported on the lack of connectivity and interoperability between databases and technologies important to the homeland security effort.[36] Databases belonging to federal law enforcement agencies and INS, for example, are not connected, and databases between state, local, and federal governments are not always connected. The technological constraints caused by different system architectures that impede the sharing of different agencies' watch lists illustrate the widespread lack of interoperability of many federal government information systems.

New technologies for data integration and interoperability could enable agencies to share information without the need for radical structural changes. This would allow the component agencies of DHS to work together yet retain a measure of autonomy, thus removing some barriers hindering agencies from embracing change. In August 2002, we reported on various existing technologies that could be more widely implemented to facilitate information sharing.[37] We reported that Extensible Markup Language (XML) is useful for better information sharing. XML is a flexible, nonproprietary set of standards for annotating or "tagging" information so

[36] GAO-02-811T
[37] U.S. General Accounting Office, *National Preparedness: Technology and Information Sharing Challenges*, GAO-02-1048R (Washington, D.C.: Aug. 30, 2002).

that it can be transmitted over a network such as the Internet and readily interpreted by disparate computer systems. If implemented broadly with consistent data definitions and structures, XML offers the promise of making it significantly easier for organizations and individuals to identify, integrate, and process information that may be widely dispersed among systems and organizations. For example, law enforcement agencies could potentially better identify and retrieve information about criminal suspects from any number of federal, state, and local databases.

We also reported that various technologies could be used to protect information in shared databases. For example, data could be protected through electronically secured entry technology (ESET). ESET would allow users of separate databases to cross check or "mine" data securely without directly disclosing their information to others, thus allowing agencies to collaborate as well as address their needs for confidentiality or privacy. Such technology could, for example, allow an airline to cross check a passenger or employee against data held by government agencies in a single-step process without actually disclosing the data to the airline. In checking an individual, the airline would not receive any data from the agencies' databases; rather, it would receive a "yes or no" type of response and/or a referral for further action. Additionally, appropriate authorities could automatically be notified.

We noted that intrusion detection systems could be used to prevent unauthorized users from accessing shared information. Intrusion detection uses normal system and network activity data as well as known attack patterns. Deviations from normal traffic patterns can help to identify potential intruders.

We also observed the need to simplify the process of analyzing information to more efficiently and effectively identify information of consequence that must be shared. Great emphasis has been placed upon data mining and data integration, but the third and perhaps most crucial component may be data visualization. The vast amount of information potentially available to be mined and integrated must be intelligently analyzed, and the results effectively presented, so that the right people have the right information necessary to act effectively upon such information. This may involve pinpointing the relevant anomalies.

Before DHS was established, the Office of Homeland Security had already begun several technological initiatives to integrate terrorist-related information from databases from different agencies responsible for homeland security. These included (1) adopting meta-data standards for electronic information so that homeland security officials understood

what information was available and where it could be found and (2) developing data-mining tools to assist in identifying patterns of criminal behavior so that suspected terrorists could be detained before they could act.

To address these technological challenges, the Homeland Security Act emphasized investments in new and emerging technologies to meet some of these challenges and established the Science and Technology Directorate, making it responsible for establishing and administering research and development efforts and priorities to support DHS missions.

Improving Information Technology Management

Improving IT management will be critical to transforming the new department. DHS should develop and implement an enterprise architecture, or corporate blueprint, to integrate the many existing systems and processes required to support its mission. This architecture will also guide the department's investments in new systems to effectively support homeland security in the coming years. Other key IT management capacities that DHS will need to establish include investment and acquisition management processes, effective IT security, and secure communications networks.

An Enterprise Architecture

Effectively managing a large and complex endeavor requires, among other things, a well-defined and enforced blueprint for operational and technological change, commonly referred to as an enterprise architecture. Developing, maintaining, and using enterprise architectures is a leading practice in engineering both individual systems and entire enterprises. Enterprise architectures include several components, including a (1) current or "as is" environment, (2) target or "to be" environment, and (3) transition plan or strategy to move from the current to the target environment. Governmentwide requirements for having and using architectures to guide and constrain IT investment decision making are also addressed in federal law and guidance.[38] Our experience with federal agencies has shown that attempts to transform IT environments without enterprise architectures often result in unconstrained investment and

[38]U.S. General Accounting Office, *Business Systems Modernization: Longstanding Management and Oversight Weaknesses Continue to Put Investments at Risk*, GAO-03-553T (Washington, D.C.: Mar. 31, 2003).

systems that are duplicative and ineffective. Moreover, our February 2002 report on the federal agencies' use of enterprise architectures found that their use of enterprise architectures was a work in progress, with much to be accomplished.[39]

DHS faces tremendous IT challenges because programs and agencies have been brought together in the new department from throughout the government, each with their own information systems. It will be a major undertaking to integrate these diverse systems to enable effective information sharing among themselves, as well as with those outside the department.

The Office of Homeland Security has acknowledged that an enterprise architecture is an important next step because it can help identify shortcomings and opportunities in current homeland-security-related operations and systems, such as duplicative, inconsistent, or missing information. Furthermore, the President's homeland security strategy identifies, among other things, the lack of an enterprise architecture as an impediment to DHS's systems interoperating effectively and efficiently. Finally, the CIO of DHS has stated that the most important function of his office will be to design and help implement a national enterprise architecture that will guide the department's investment in and use of IT. As part of its enterprise development efforts, the department has established working groups comprising state and local CIOs to ensure that it understands and represents their business processes and strategies relevant to homeland security. In addition, OMB, in its current review of DHS's redundant IT for consolidation and integration, has taken an initial first step to evaluate DHS's component systems.[40] According to an official in the office of the CIO, DHS has compiled an inventory of systems that represents its current enterprise architecture and will soon have a draft of its future enterprise architecture. In addition, this official anticipates having a preliminary road map of the plan to transition to the future enterprise architecture in September 2003 and estimates that DHS will have the plan itself by next winter.

In June 2002, we recommended that the federal government develop an architecture that defined the homeland security mission and the information, technologies, and approaches necessary to perform the mission in a way that was divorced from organizational parochialism and

[39]U.S, General Accounting Office, *Information Technology: Enterprise Architecture Use across the Federal Government Can Be Improved*, GAO-02-6 (Washington, D.C.: Feb. 19, 2002).
[40]Office of Management and Budget, *Reducing Redundant IT Infrastructure Related to Homeland Security, Memorandum for the Heads of Selected Departments and Agencies*, July 19, 2002, M-02-12.

cultural differences.[41] Specifically, we recommended that the architecture describe homeland security operations in both (1) logical terms, such as interrelated processes and activities, information needs and flows, and work locations and users; and (2) technical terms, such as hardware, software, data, communications, and security attributes and performance standards. We observed that a particularly critical function of a homeland security architecture would be to establish protocols and standards for data collection to ensure that data being collected were usable and interoperable and to tell people what they needed to collect and monitor.

The CIO Council, OMB, and GAO have collaborated to produce guidance on the content, development, maintenance, and implementation of architectures that could be used in developing an architecture for DHS.[42] In April, we issued an executive guide on assessing and improving enterprise architecture management that extends this guidance.[43]

Investment and Acquisition Management Processes

The Clinger-Cohen Act, federal guidance, and recognized best practices provide a framework for organizations to follow to effectively manage their IT investments. This involves having a single, corporate approach governing how an organization's IT investment portfolio is selected, controlled, and evaluated across its various components, including assuring that each investment is aligned with the organization's enterprise architecture. The lack of effective processes can lead to cost, schedule, and performance shortfalls, and in some cases, to failed system development efforts. We have issued numerous reports on investment and acquisition management challenges at agencies now transferred into DHS, including INS.

INS has had long-standing difficulty developing and fielding information systems to support its program operations. Since 1990, we have reported that INS managers and field officials did not have adequate, reliable, and timely information to effectively carry out the agency's mission. For example, INS's benefit fraud investigations have been hampered by a lack

[41]GAO-02-811T.
[42]See Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0, (Washington, D.C.: Feb. 2001).
[43]U.S. General Accounting Office, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, GAO-03-584G (Washington, D.C.: April 2003).

of integrated information systems.[44] Also, INS's alien address information could not be fully relied on to locate many aliens who were believed to be in the country and who might have knowledge that would assist the nation in its antiterrorism efforts.[45] Contributing to this situation was INS's lack of written procedures and automated controls to help ensure that reported changes of address by aliens are recorded in all of INS's automated databases. Our work has identified weaknesses in INS's IT management capacities as the root cause of its system problems, and we have made recommendations to correct the weaknesses. INS has made progress in addressing our recommendations.

In his written statement for a May 2003 hearing before the House Government Reform Committee, the DHS CIO stated that IT investments, including mission-specific investments, are receiving a departmentwide review. Benefits envisioned from this capital investment and control process include integrating information and identify and eliminating duplicate applications, gaps in information, and misalignments with business goals and objectives.

Sound acquisition management is also central to accomplishing the department's mission. One of the largest federal departments, DHS will potentially have one of the most extensive acquisition requirements in government. The new department is expected to acquire a broad range of technologies and services from private-sector companies.

Moreover, DHS is faced with the challenge of integrating the procurement functions of many of its constituent programs and missions. Inherited challenges exist in several of the incoming agencies. For example, Customs has major procurement programs under way that must be closely managed to ensure that it achieves expectations. Despite some progress, we reported that Customs still lacks important acquisition management controls.[46] For its new import processing system, Customs has not begun to establish process controls for determining whether acquired software products and services satisfy contract requirements before acceptance, nor to establish related controls for effective and efficient transfer of acquired software products to the support organization responsible for

[44]U.S. General Accounting Office, *Immigration Benefit Fraud: Focused Approach Is Needed to Address Problems*, GAO-02-66 (Washington, D.C.: Jan. 31, 2002).
[45]U.S. General Accounting Office, *Homeland Security: INS Cannot Locate Many Aliens Because It Lacks Reliable Address Information*, GAO-03-188 (Washington, D.C.: Nov. 21, 2002).
[46]U.S. General Accounting Office, *Customs Service Modernization: Management Improvements Needed on High-Risk Automated Commercial Environment Project*, GAO-02-545 (Washington, D.C.: May 13, 2002).

software maintenance. Agreeing with one of our recommendations, Customs continues to make progress and plans to establish effective acquisition process controls.

Getting the most from its IT investment will depend on how well the department manages its acquisition activities. High-level attention to strong system and service acquisition management practices is critical to ensuring success.

Information Security Challenges

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency, and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.[47] Further, the Homeland Security Act specifically requires DHS to establish procedures to ensure the authorized use and the security and confidentiality of information shared with the department, including information on threats of terrorism against the United States; infrastructure or other vulnerabilities to terrorism; and threatened interference with, attack on, compromise of, or incapacitation of critical infrastructures or protected systems by either physical or computer-based attack. However, establishing an effective information security program may present significant challenges for DHS, which must bring together programs and agencies from throughout the government and integrate their diverse communications and information systems to enable effective communication and information sharing both within and outside the department.

Since 1996, we have reported that poor information security is a widespread problem for the federal government, with potentially devastating consequences.[48] Further, we have identified information security as a governmentwide high-risk issue in reports to the Congress

[47] *Title III—Federal Information Security Management Act of 2002*, *E-Government Act of 2002*, P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002.
[48] U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

since 1997—most recently in January 2003.[49] Although agencies have taken steps to redesign and strengthen their information system security programs, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. For the past several years, we have analyzed audit results for 24 of the largest federal agencies,[50] and our latest analyses, of audit reports issued from October 2001 through October 2002, continued to show significant weaknesses in federal computer systems that put critical operations and assets at risk.[51] In particular, we found that all 24 agencies had weaknesses in security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls and covers a range of activities related to understanding information security risks, selecting and implementing controls commensurate with risk, and ensuring that the controls implemented continue to operate effectively. In addition, we found that 22 of the 24 agencies had weaknesses in access controls—weaknesses that can make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage, or in today's increasingly interconnected computing environment, can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise. In April 2003,[52] we also reported that many agencies still had not established information security programs consistent with requirements originally prescribed by government information security reform legislation[53] and now permanently authorized by FISMA.

Considering the sensitive and classified information to be maintained and shared by DHS, it is critical that the department implement federal

[49]U.S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).
[50]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000); *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001), and *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk*, GAO-02-303T (Washington, D.C.: Nov. 19, 2002).
[51]GAO-03-303T.
[52]GAO-03-564T.
[53]*Title X, Subtitle G—Government Information Security Reform*, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L.106-398, October 30, 2000.

information security requirements to ensure that its systems are appropriately assessed for risk and that adequate controls are implemented and working properly. Federal information security guidance, such as that issued by the National Institute of Standards and Technology (NIST), can aid DHS in this process. For example, NIST has issued guidance to help agencies perform self-assessments of their information security programs, conduct risk assessments, and use metrics to determine the adequacy of in-place security controls, policies, and procedures.[54] In addition, as we have previously reported, agencies need more specific guidance on the controls that they need to implement to help ensure adequate protection.[55] Currently, agencies have wide discretion in deciding which computer security controls to implement and the level of rigor with which to enforce these controls. Although one set of specific controls will not be appropriate for all types of systems and data, our studies of best practices at leading organizations have shown that more specific guidance is important.[56] In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately protected; and reduce demands for limited resources to independently develop security controls. Responding to this need, FISMA requires NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

DHS has identified implementing its information security program as a year-one objective. In continuing these efforts, it is important that DHS consider establishing processes to annually review its information security program and to collect and report data on the program, as required by FISMA and OMB.

[54]National Institute of Standards and Technology, *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication 800-26, November 2001; *Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards and Technology*, Special Publication 800-30, January 2002; *Security Metrics Guide for Information Technology Systems*, NIST Draft Special Publication 800-55 (October 2002).
[55]GAO-03-121.
[56]U.S. General Accounting Office, *Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

Secure Communications Networks

The Homeland Security Information Sharing Act, included in the Homeland Security Act of 2002, provides for the President to prescribe and implement procedures for federal agencies to share homeland security and classified information with others, such as state and local governments, through information sharing systems. Provisions of the act depict the type of information to be shared as that which reveals a threat of actual or potential attack or other hostile acts. Grand jury information; electronic, wire, or oral information; and foreign intelligence information are all included in these provisions. The *National Strategy for Homeland Security* also refers to the need for states to use a secure intranet to increase the flow of classified federal information to state and local entities. According to the strategy, this network would provide a more effective way to share information about terrorists. The strategy also refers to putting into place a "collaborative classified enterprise environment" to allow agencies to share information in their existing databases.

To ensure the safe transmittal of sensitive, and, in some cases, classified, information vertically among everyone from intelligence entities, including the CIA, to local entities, such as those involved in emergency response and law enforcement, as well as horizontally across the same levels of government, requires developing and implementing communications networks with adequate security to protect the confidentiality, integrity, and availability of the transmitted information. Furthermore, these communications networks must be accessible to a variety of parties, from federal agencies to state and local government entities and some private entities.

Secure networks for sharing sensitive information between state and federal entities have been implemented and are being used. For example, the National Law Enforcement Telecommunication System (NLETS) links all states and many federal agencies to the FBI's National Crime Information Center (NCIC) network for the exchange of criminal justice information. Another law enforcement system called the Regional Information Sharing System (RISS) links thousands of local, state, and federal agencies to Regional Organized Crime Information Centers. Information sharing networks for the purpose of sharing sensitive information with some federal agencies also exist within the intelligence community. Other agencies are also engaged in efforts to provide homeland security networking and information management support for crisis management activities. Department of Defense officials have also stated that the Army National Guard's network GuardNet, which was used

to communicate among the states and the District of Columbia during the September 11 terrorist attacks, is being considered for homeland security mission support. For several years, the states have also been working on efforts to establish an information architecture framework for government information systems integration.

There also appear to be many new efforts under way to implement secure networks. In addition, according to the recently published the cyberspace security strategy, DHS intends to develop a national cyberspace security response system, the Cyber Warning Information Network (CWIN), to provide crisis management support to government and nongovernment network operation centers. CWIN is envisioned as providing private and secure network communications for both government and industry for the purpose of sharing cyber alert and warning information. Moreover, the National Communications System, one of the 22 entities that were merged into the DHS, has implemented a pilot system, the Global Early Warning Information System (GEWIS), which will measure how critical areas of the Internet are performing worldwide and then use that data to notify government, industry, and allies of impending cyber attacks or possible disturbances.

It was also recently reported that the Justice Department and the FBI are expanding two existing sensitive but unclassified law enforcement networks to share homeland security information across all levels of government. When fully deployed, their Antiterrorism Information Exchange (ATIX) will provide law enforcement agencies at all levels access to information. Law enforcement agencies also can use ATIX to distribute security alerts to private-sector organizations and public officials who lack security clearances. Users, who will have different access levels on a need-to-know basis, will include a broad range of public safety and infrastructure organizations, including businesses that have homeland security concerns and duties. They will have access to a secure E-mail system via a secure Intranet, which the FBI and DHS will use to deliver alerts to ATIX users. The FBI and other federal agencies, including DHS, will link to ATIX via Law Enforcement Online, the bureau's system for sensitive-but-unclassified law enforcement data that provides an encrypted communications service for law enforcement agencies on a virtual private network. The second Department of Justice and FBI network, the Multistate Antiterrorism Regional Information Exchange System, will enable crime analysts working on terrorism investigations to quickly check a broad range of criminal databases maintained by federal, state, and local agencies.

DHS reportedly is establishing secure videoconferencing links with emergency operations centers in all 50 states, as well as two territories and the District of Columbia. Also, the DHS CIO has stated that a major initiative in implementing the department's IT strategy for providing the right information to the right people at all times is establishing the DHS Information Sharing Network Pilot project. Moreover, he sets 2005 as a milestone for DHS to build a "network of networks." However, at this time, we do not have information on these projects or the extent to which they will rely on existing networks. It is also not clear how the DHS "network of networks" architecture will work with the state architecture being developed by the National Association of State CIOs.

Managing Performance

As we have previously reported,[57] the new department has the challenge of developing a national homeland security performance focus, which relies on related national and agency strategic and performance planning efforts of the Office of Homeland Security, OMB, and the other departments and agencies. Indeed, the individual planning activities of the various component departments and agencies represent a good start in the development of this focus. However, our past work on implementation of the Government Performance and Results Act (GPRA) has highlighted ongoing difficulty with many federal departments and agencies setting adequate performance goals, objectives, and targets. Accordingly, attention is needed to developing and achieving appropriate performance expectations and measures for information sharing and in ensuring that there is linkage between DHS's plans, other agencies' plans, and the national strategies regarding information sharing. Ensuring these capabilities and linkages will be vital in establishing comprehensive planning and accountability mechanisms that will not only guide DHS's efforts but also help assess how well they are really working.

As we previously reported,[58] one of the barriers that the new department faces in establishing effective homeland security is interagency cooperation, which is largely attributed to "turf" issues among the 22 component agencies subsumed by the new department. Strong and sustained commitment of agency leaders would provide performance incentives to managers and staff to break down cultural resistance and

[57]U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: January 2003).
[58]*GAO-02-1048R*.

encourage more effective information sharing pertaining to homeland security. Moreover, agency leaders have a wide range of tools at their disposal for enforcing and rewarding cooperative efforts, including performance bonuses for senior executives and incentive award programs for staff.

Our studies of other cross-cutting federal services with similar "turf" problems have also shown that agency performance plans, which are required by GPRA, offer a good avenue for developing incentives to cooperate. Specifically, agencies can set up goals in their performance plans for participation in cross-cutting programs and report on their progress in meeting these goals to the Congress. The Congress could also build similar incentives into budget resolutions.

Shared programmatic goals and metrics would also encourage cooperation and coordination. Agencies subsumed by DHS should all participate in the development of goals, milestones, and metrics to measure progress and success, and such indicators should be clearly articulated and endorsed by senior management. Such goals and metrics must be carefully chosen since how performance is measured greatly influences the nature of the performance itself; poorly chosen metrics may lead to unintended or counterproductive results. However, visible, clearly articulated and carefully chosen shared goals and metrics can effectively overcome "turf" issues. Developing metrics to measure the success of these activities is critical to ensuring a successful effort. Similar indicators more directly related to information sharing could be developed.

Emphasizing Human Capital

Human capital is another critical ingredient required for ensuring successful information sharing for homeland security. The cornerstones to effective human capital planning include leadership; strategic human capital planning; acquiring, developing, and retaining talent; and building results-oriented organizational cultures. The homeland security and intelligence communities must include these factors in their management approach in order to benefit from effective collaboration in this critical time.

As we have previously reported, the governmentwide increase in homeland security activities has created a demand for personnel with skills in areas such as IT, foreign language proficiencies, and law enforcement, without whom critical information has less chance of being shared, analyzed, integrated, and disseminated in a timely, effective

manner.[59] We specifically reported that shortages in staffing at some agencies had exacerbated backlogs in intelligence and other information, adversely affecting agency operations and hindering U.S. military, law enforcement, intelligence, counterterrorism, and diplomatic efforts.[60]

We have also previously reported that some of the agencies that moved into DHS have long-standing human capital problems that will need to be addressed. One of these challenges has been the ability to hire and retain a talented and motivated staff. For example, we reported that INS has been unable to reach its program goals in large part because of such staffing problems as hiring shortfalls and agent attrition.[61] We also reported that several INS functions have been affected by the lack of a staff resource allocation model to identify staffing needs.[62] We concluded then that it was likely that increased attention to the enforcement of immigration laws and border control would test the capacity of DHS to hire large numbers of inspectors for work at our nation's border entry points. Moreover, we reported that other agencies being integrated into DHS were also expected to experience challenges in hiring security workers and inspectors. For example, we reported that the Agriculture Department, the Customs Service, INS, and other agencies were all simultaneously seeking to increase the size of their inspections staffs.[63]

To overcome its significant human capital shortfalls, DHS must develop a comprehensive strategy capable of ensuring that the new department can acquire, develop, and retain the skills and talents needed to prevent and protect against terrorism. This requires identifying skill needs; attracting people with scarce skills into government jobs; melding diverse compensation systems to support the new department's many needs; and establishing a performance-oriented, accountable culture that promotes employee involvement and empowerment. In February, the DHS CIO acknowledged the lack of properly skilled IT staff within the component agencies. Challenges facing DHS in this area, he stated, include overcoming political and cultural barriers, leveraging cultural beliefs and diversity to achieve collaborative change, and recruiting and retaining skilled IT workers. He acknowledged that the department would have to evaluate the talent and skills of its IT workforce to identify existing skill

[59]GAO-02-1122T.
[60]U.S. General Accounting Office, *Foreign Languages: Human Capital Approach Needed to Correct Staffing and Proficiency Shortfalls*, GAO-02-375 (Washington, D.C.: January 2002).
[61]U.S. General Accounting Office, *Immigration Enforcement: Challenges to Implementing the INS Interior Enforcement Strategy*, GAO-02-861T (Washington, D.C.: June 19, 2002).
[62]U.S. General Accounting Office, *Immigration and Naturalization Service: Overview of Recurring Management Challenges*, GAO-02-168T (Washington, D.C.: Oct. 17, 2001).
[63]GAO-03-260.

gaps. He further stated that a critical component of DHS's IT strategic plan would address the actions needed to train, reskill, or acquire the necessary skills to achieve a world-class workforce. He committed to working closely with the department's Chief Human Capital Officer and with the Office of Personnel Management to achieve this goal. He set July 2003 as a milestone for developing a current inventory of IT skills, resources, and positions and September 2003 as the targeted date for developing an action plan.

Ensuring Institutional Oversight

It is important to note that accountability is also a critical factor in ensuring the success of the new department. The oversight entities of the executive branch—including the inspectors general, OMB, and the Office of Homeland Security—have a vital role to play in ensuring expected performance and accountability. Likewise, congressional committees and GAO, as the investigative arm of the legislative branch, with their long-term and broad institutional roles, also have roles to play in overseeing that the new department meets the demands of its homeland security mission.

– – – –

In summary, information sharing with and between all levels of government and the private sector must become an integral part of everyday operations if we are to be able to identify terrorist threats and protect against attack. As such, information sharing is an essential part of DHS's responsibilities and is critical to achieving its mission. To implement these responsibilities, DHS will need to develop effective information sharing systems and other information sharing mechanisms. The department will also need to develop strategies to address other challenges in establishing its organization and information architecture and in developing effective working relationships, cooperation, and trust with other federal agencies, state and local governments, and the private sector.

Messrs. Chairmen, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittees may have at this time.

Contacts and Acknowledgements

For information about this statement, please contact Robert Dacey, Director, Information Security Issues, at (202) 512-3317, or William Ritt, Assistant Director, at (202) 512-6443. You may also reach them by E-mail at daceyr@gao.gov or rittw@gao.gov. Individuals who made key contributions to this testimony include Mark Fostek, Sophia Harrison, and Barbarol James.

(310510)

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