United States General Accounting Office

GAO

January 2003

High-Risk Series

Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures

GAO-03-121

This Series

This report on protecting information systems supporting the federal government and the nation's critical infrastructures is part of GAO's high-risk series, first issued in 1993 and updated periodically. This series identifies areas at high risk due to either their greater vulnerabilities to waste, fraud, abuse, and mismanagement or major challenges associated with their economy, efficiency, or effectiveness. A companion series entitled the *Performance and Accountability Series: Major Management Challenges and Program Risks* contains separate reports covering each cabinet department, most major independent agencies, and the U.S. Postal Service. The series also includes a governmentwide perspective on transforming the way the government does business in order to meet 21st century challenges and address long-term fiscal needs. A list of all of the reports in this series is included at the end of this report.

January 2003

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of a high-risk area discussed later in this report (GAO-03-121)

HIGH-RISK SERIES

Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures

Why Area Is High Risk

Since GAO designated computer security in the federal government as high risk in 1997, evidence of pervasive weaknesses has been continuing. Also, related risks have been escalating, in part because of the dramatic increases in computer interconnectivity and increasing dependence on computers to support critical operations and infrastructures, such as power distribution, water supply, national defense, and emergency services. This year, GAO expanded this high risk area to include protecting the information systems that support our nation's critical infrastructures, referred to as cyber critical infrastructure protection or cyber CIP. Among other reasons for designating cyber CIP high risk is that terrorist groups and others have stated their intentions of attacking our critical infrastructures, and failing to protect these infrastructures could adversely affect our national security, economic security, and/or public health and safety.

What Remains to Be Done

Among other actions essential to sustaining federal information security improvements are the agencies' development of effective risk management programs and the development of a comprehensive strategy to guide agencies' efforts. Further actions to improve CIP include developing a national CIP strategy and improving analysis and warning capabilities and information sharing on threats and vulnerabilities.

www.gao.gov/cgi-bin/getrpt?GAO-03-121.

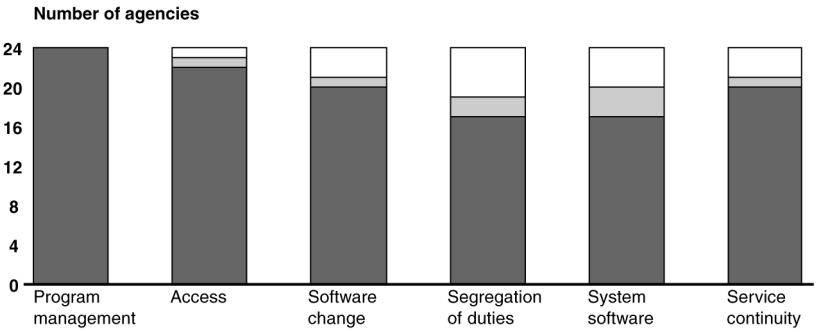
For additional information about this high-risk area, click on the link above or contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

What GAO Found

Since January 2001, efforts to improve federal information security have accelerated at individual agencies and at the governmentwide level. For example, implementation of Government Information Security Reform legislation (GISRA) enacted by the Congress in October 2000 was a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. In implementing GISRA, agencies have noted benefits, including increased management attention to and accountability for information security. Although improvements are under way, recent audits of 24 of the largest federal agencies continue to identify significant information security weaknesses that put critical federal operations and assets in each of these agencies at risk (see figure below).

Over the years, various working groups have been formed, special reports written, federal policies issued, and organizations created to address the nation's critical infrastructure challenges. In 1998, the President issued Presidential Decision Directive 63 (PDD 63), which 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 designated and established organizations to provide central coordination and support. This directive has since been supplemented by Executive Order 13231, which established the President's Critical Infrastructure Protection Board and the President's *National Strategy for Homeland Security*. While the actions taken to date are major steps to more effectively protect our nation's critical infrastructures, GAO has made numerous recommendations over the last several years concerning CIP challenges. In response to these challenges, improvements have been made and efforts are in progress, but more work is needed to address them.

Information Security Weaknesses at 24 Major Agencies



Source: Audit reports issued October 2001 through October 2002.

Contents

United States General Accounting Office
Washington, D.C. 20548

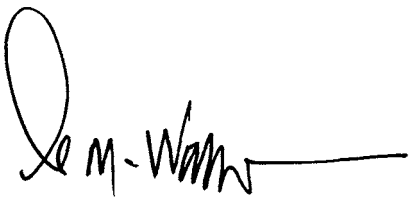
January 2003

The President of the Senate
The Speaker of the House of Representatives

GAO's high-risk update is provided at the start of each new Congress in conjunction with a special series GAO has issued biennially since January 1999, entitled the *Performance and Accountability Series: Major Management Challenges and Program Risks.* This report, which discusses information security in the federal government and our nation's critical infrastructures (such as power distribution, water supply, national defense, and emergency services), is a companion to GAO's 2003 high-risk update, *High-Risk Series: An Update* (GAO-03-119). These reports are intended to help the new Congress focus its attention on the most important issues and challenges facing the federal government.

Significant, pervasive information security weaknesses continue to put critical federal operations and assets at high risk. This year, GAO expanded this high-risk area to include protecting the information systems that support our nation's critical infrastructures, referred to as cyber critical infrastructure protection or cyber CIP. Among other reasons for designating cyber CIP high risk is that terrorist groups and others have stated their intentions of attacking our critical infrastructures, and failing to adequately protect these infrastructures could adversely affect our national security, national economic security, and/or national public health and safety.

This report should help the new Congress and the administration attend to these problems and improve the federal government's efforts concerning information security and critical infrastructure protection for the benefit of the American people. For additional information about this report, please contact Robert F. Dacey, Director, Information Security Issues, at (202) 512-3317.



David M. Walker
Comptroller General
of the United States

Protecting Information Systems: A High-Risk Area

Since 1997, we have designated information security as a governmentwide high-risk issue because of continuing evidence indicating significant, pervasive weaknesses in the controls over computerized federal operations. Moreover, related risks continue to escalate, in part due to the government's increasing reliance on the Internet and on commercially available information technology. In addition, we continue to report significant information security weaknesses in 24 major federal agencies.[1] Since our last high-risk report, agencies and the administration have taken actions to identify and correct information security weaknesses and to strengthen federal information security, including implementing government information security reform legislation enacted by the Congress in October 2000 (commonly referred to as "GISRA") and developing guidance and tools for agencies to perform self-assessments of their information security programs. However, although improvements are under way, recent audits continue to show that federal operations and assets are highly vulnerable to computer-based attacks. On December 17, 2002, the Federal Information Security Management Act of 2002 was enacted, which permanently authorizes and strengthens the information security program, evaluation, and reporting requirements established by GISRA.

In our January 2001 high-risk update report, we also began to highlight the increasing importance of the federal government's efforts to protect our nation's critical public and private computer-dependent infrastructure (such as national defense, power distribution, and water supply), as outlined in Presidential Decision Directive 63 (PDD 63). This year, we are expanding this high-risk issue to emphasize the increased importance of protecting the information systems that support these critical infrastructures, referred to as cyber critical infrastructure protection or cyber CIP. Since our 2001 report, terrorist attacks and threats have further underscored the need to manage CIP activities that enhance the security of those cyber and physical public and private infrastructures that are essential to national security, national economic security, and/or national public health and safety. At the federal level, cyber CIP activities are perhaps the most critical component of a department or agency's overall information security program. In addition, although the government has

[1]U.S. General Accounting Office, *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-03-303T (Washington, D.C.: Nov. 19, 2002).

made steady progress in working with the private sector to better secure critical infrastructures, this issue should be designated as part of our information security high-risk issue because

- failure to adequately protect these infrastructures could have consequences for national security, national economic security, and/or national public health and safety;
- terrorist groups and others have stated their intentions of attacking our critical infrastructures;
- federal influence over the private sector's management of our nation's critical infrastructures poses unique challenges; and
- further actions on GAO's CIP recommendations are needed, including (1) developing a national CIP strategy, (2) improving analysis and warning capabilities, and (3) improving information sharing on threats and vulnerabilities.

Cyber Threats Are Increasing

Dramatic increases in computer interconnectivity, especially in the use of the Internet, are revolutionizing the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often on a 24-hour-a-day basis; and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups.

In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, and national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. Likewise, the speed and accessibility that create the enormous benefits of the computer age, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these

operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

Government officials are increasingly concerned about attacks launched by individuals and groups with malicious intents, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the Federal Bureau of Investigation (FBI), terrorists, transnational criminals, and intelligence services are quickly becoming aware of and 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. 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 information technology, the likelihood increases that information attacks will threaten vital national interests. In addition, the disgruntled organization insider is a significant threat, since such 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.

Reports of attacks and disruptions abound. The 2002 report of the "Computer Crime and Security Survey," conducted by the Computer Security Institute and the FBI's San Francisco Computer Intrusion Squad, showed that 90 percent of respondents (primarily large corporations and government agencies) had detected computer security breaches within the last 12 months. In addition, the number of computer security incidents reported to the CERT® Coordination Center[2] rose from 9,859 in 1999 to 52,658 in 2001 and 82,094 in 2002. And these are only the reported attacks. The Director, 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.

[2]CERT Coordination Center is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

Since the September 11, 2001, attacks, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, in July 2002, the FBI's National Infrastructure Protection Center (NIPC) reported that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure. As NIPC reported, the effects of a swarming attack include slowing or complicating the response to a physical attack. Also, earlier this year, the Special Advisor to the President for Cyberspace Security stated in a Senate briefing that although to date none of the traditional terrorist groups such as al Qaeda have used the Internet to launch a known attack on the U.S. infrastructure, information on computerized water systems was recently discovered on computers found in al Qaeda camps in Afghanistan. Further, in his October 2001 congressional testimony, former Virginia Governor James Gilmore warned that systems and services critical to the American economy and the health of our citizens—such as banking and finance, "just-in-time" delivery systems for goods, hospitals, and state and local emergency services—could all be shut down or severely handicapped by a cyber attack or a physical attack against computer hardware.[3]

Important Actions Taken to Improve Federal Information Security

Since January 2001, efforts to improve federal information security have accelerated both at individual agencies and at the governmentwide level.

- Several agencies, including the Departments of Commerce, Defense, Education, and the Interior, have taken actions to improve their information security programs stemming from recommendations in prior years' audits and recent follow-up work. For example, Commerce officials have shown a commitment to correcting vulnerabilities identified in our August 2001 report.[4] They indicate that they have developed and implemented an action plan for strengthening access controls for the department's sensitive systems; published policy on comprehensive recovery plans that applies to all Commerce operating units to help ensure continuity of operations; and begun the process of

[3]Testimony of James S. Gilmore III, Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction (commonly known as the "Gilmore Commission"), before the House Science Committee, October 17, 2001.

[4]U.S. General Accounting Office, *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*, GAO-01-751 (Washington, D.C.: Aug. 13, 2001).

establishing a departmentwide incident-handling capability with formal procedures for preparing for, detecting, responding to, and reporting incidents. Although neither the department's inspector general nor GAO has yet validated these corrective actions, these responses show that the agency is attempting to quickly address identified weaknesses.

- Implementation of Government Information Security Reform legislation enacted by the Congress in October 2000 (commonly referred to as "GISRA") has been a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses.[5] GISRA consolidates federal information security requirements found in law and guidance into an overall management framework covering all agency systems, adds new statutory evaluation and reporting requirements that facilitate implementation of these requirements, and strengthens Office of Management and Budget (OMB) and congressional oversight. In implementing GISRA, agencies noted benefits, including increased management attention to and accountability for information security. In addition, GISRA implementation resulted in important actions by the administration that, if properly implemented, should continue to improve information security in the federal government. For example, OMB has issued guidance that information technology investments will not be funded unless security is incorporated into and funded as part of each investment. The administration also has plans to

  - direct all large agencies to undertake a review to identify and prioritize their critical infrastructure assets and the interrelationships of these assets with those of other agencies and the private sector, and

  - integrate security into the President 's Management Agenda Scorecard.

- As part of its responsibilities to oversee the implementation of GISRA, OMB has created an annual reporting process requiring that, in addition to reporting the results of their independent evaluations as required by GISRA, agencies submit annual reports on the status of their efforts to implement security policies and procedures, as well as corrective action

[5]Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L. 106-398, Oct. 30, 2000.

plans to track progress in correcting identified weaknesses. Further, as part of its guidance for fiscal year 2002 GISRA reporting, OMB provided agencies with specific performance measures for agency officials who are accountable for information and information-technology security.

- The National Institute of Standards and Technology (NIST) developed a Security Self-Assessment Guide and supporting tools to help agencies perform self-assessments of their information security programs.[6] This guide accompanies NIST's Security Assessment Framework methodology, which agency officials can use to determine the current status of their security programs.[7] The guide itself uses an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. Many agencies used a draft version of the self-assessment guide for their fiscal year 2001 GISRA program reviews, and with issuance of a final version in November 2001, OMB now requires that the guide be used for fiscal year 2002 reviews. Also, to automate the completion of the questionnaire, NIST developed a tool that can be found at its Computer Security Resource Center Web site: http://csrc.nist.gov/asset/.

- During 2001 and 2002, the Congress continued to hold important hearings on progress at specific agencies and on ways to strengthen information security practices throughout the federal government and to better address threats to the nation's critical computer-dependent infrastructures. In addition, the Congress considered a number of bills related to information security, including those that would permanently authorize GISRA. On December 17, 2002, the Federal Information Security Management Act of 2002 was enacted as title III of the E-Government Act of 2002. The Federal Information Security Management Act permanently authorizes and strengthens the information security program, evaluation, and reporting requirements established by GISRA. Among its other provisions, it also requires NIST to develop standards that provide mandatory minimum information security requirements for federal information systems.

[6]National Institute of Standards and Technology, *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication 800-26, November 2001.

[7]National Institute of Standards and Technology, *Federal Information Technology Security Assessment Framework*, prepared for the Federal CIO Council by the NIST Computer Security Division Systems and Network Security Group, Nov. 28, 2000.

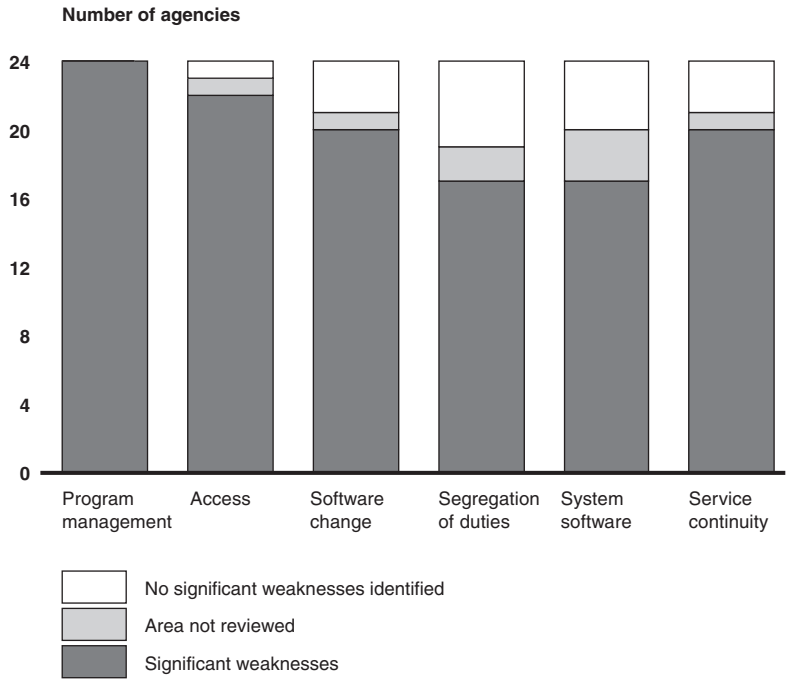
Continuing Federal Information Security Weaknesses Underscore the Need for Further Action

In both 2001 and 2002, we continued our analyses of audit reports for 24 major departments and agencies and identified significant information security weaknesses in each that put critical federal operations and assets at risk.[8] These weaknesses were found in all six major areas of agencies' general controls, that is, the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions.

Our most recent analyses showed that weaknesses were most often identified for security program management and access controls. For security program management, we identified weaknesses for all 24 agencies in 2002—the same as reported for 2001. For access controls, we identified weaknesses for 22 of 24 agencies (92 percent) in 2002, as compared to weaknesses reported for all 24 agencies in 2001. Figure 1 illustrates the distribution of information security weaknesses for all six general control areas across the 24 agencies for our 2002 analyses.

[8]GAO-03-303T.

Figure 1: Information Security Weaknesses at 24 Major Agencies



Source: Audit reports issued October 2001 through October 2002.

Recently reported findings for individual agencies include the following examples:

- In February 2002, we reported that the Internal Revenue Service (IRS) corrected or mitigated many of the computer security weaknesses identified in our previous reports, but much remains to be done to resolve the significant control weaknesses that continue to exist within IRS's computing environment and to be able to promptly address new security threats and risks as they emerge.[9] Weaknesses found, such as not always adequately restricting electronic access within its computer networks and to its systems, can impair the agency's ability to perform vital functions and increase the risk that unauthorized individuals could gain access to critical hardware and software and intentionally or inadvertently view, alter, or delete sensitive data or computer programs.

[9]U.S. General Accounting Office, *Financial Audit: IRS's Fiscal Year 2001 and 2000 Financial Statements*, GAO-02-414 (Washington, D.C.: Feb. 27, 2002).

These weaknesses also increase the risk that unauthorized individuals could obtain personal taxpayer information and use it to commit financial crimes in taxpayers' names (identity fraud), such as establishing credit and incurring debt. In response to our findings, IRS initiated actions to correct identified weaknesses, including improving the monitoring of key systems to identify unauthorized activities.

- In April 2002, the inspector general for the Department of Justice reported serious deficiencies in controls for five sensitive-but-unclassified systems that support critical departmental functions, such as tracking prisoners; collecting, processing, and disseminating unclassified intelligence information; and providing secure information technology facilities, computing platforms, and support services. The most significant of these deficiencies concerned the technical controls that help prevent unauthorized access to system resources. Because of the repetitive nature of the security deficiencies and concerns identified, the inspector general recommended that a central office responsible for system security be established to identify trends and enforce uniform standards. The inspector general also included other specific recommendations intended to improve departmentwide computer security for both classified and sensitive-but-unclassified systems. In addition to this report, in March 2002, the Commission for Review of FBI Security Programs reported that the FBI's information systems security controls were inadequate.

- In June 2002, we reported that the U.S. Army Corps of Engineers had made substantial progress in improving computer controls at each of its data processing centers and other Corps sites since our 1999 review, but that continuing and numerous newly identified control vulnerabilities continued to impair the Corps' ability to ensure the reliability, confidentiality, and availability of financial and sensitive data.[10] These vulnerabilities warranted management's attention in order to decrease the risk of inappropriate disclosure and modification of data and programs, misuse of or damage to computer resources, or disruption of critical operations. These vulnerabilities also increased risks to other Department of Defense (DOD) networks and systems to which the Corps' network is linked. The Corps indicated that it has completed corrective action on some of the open and new recommendations and

[10]U.S. General Accounting Office, *Information Security: Corps of Engineers Making Improvements, But Weaknesses Continue*, GAO-02-589 (Washington, D.C.: June 10, 2002).

has developed an action plan to address the remaining recommendations.

- In a September 2002 testimony, we reported that the Department of Veterans Affairs had taken important steps to strengthen its computer security management program, including increasing security training; providing a more solid foundation for detecting, reporting, and responding to security incidents; and reducing the risk of unauthorized access through external connections to its critical systems.[11] Nonetheless, the department had not yet fully implemented a comprehensive computer security management program that included a process for routinely monitoring and evaluating the effectiveness of security policies and controls and addressing identified vulnerabilities. Further, the department's offices were self-reporting computer security weaknesses, and the department lacked an independent component to ensure the accuracy of reporting and validating corrective actions taken. In addition to our findings and those of the inspector general, the department itself has self-reported approximately 27,000 computer security weaknesses since September 2001. As of the end of August 2002, about half of these weaknesses (14,000) remained unresolved.

- In addition to individual agency reports, in its February 2002 report to the Congress on GISRA, OMB noted that although examples of good security exist in many agencies, and others are working very hard to improve their performance, many agencies have significant deficiencies in every important area of security.[12] In particular, the report highlighted six common security weaknesses:

  - a lack of senior management attention to information security;
  - inadequate accountability for job and program performance related to information technology security;
  - limited security training for general users, information technology professionals, and security professionals;

[11]U.S. General Accounting Office, *VA Information Technology: Management Making Important Progress in Addressing Key Challenges*, GAO-02-1054T (Washington, D.C.: Sept. 26, 2002).

[12]Office of Management and Budget, *FY 2001 Report to Congress on Federal Government Information Security Reform*, February 2002.

- inadequate integration of security into the capital planning and investment control process;
- poor security for contractor-provided services; and
- limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections.

Further Actions Needed to Improve Federal Information Security

Recent audits and reviews, including annual GISRA program reviews and independent evaluations, show that although agencies have made progress in addressing GAO and inspector general recommendations to improve the effectiveness of their information security, further action is needed. In particular, overall security program management continues to be an area marked by widespread and fundamental problems.

Many agencies have not developed security plans for major systems based on risk, have not documented security policies, and have not implemented a program for testing and evaluating the effectiveness of the controls they rely on. As a result, they could not ensure that the controls they had implemented were operating as intended and they could not make informed judgments as to whether they were spending too little or too much of their resources on security.

With the enactment of GISRA in October 2000, agencies were formally required to adopt risk management practices. Our May 1998 guide provides a roadmap for managing risks through an ongoing cycle of activities coordinated by a central focal point and is widely adopted throughout the federal government.[13] In November 1999, we also issued a supplement to this guide that provides additional direction on risk assessment, including a list of critical success factors and examples of practical risk assessment procedures that have been successfully adopted by leading organizations.[14] In addition to this GAO guidance, in January 2002, NIST issued a risk management guide to provide a foundation for the development of an effective risk management program.[15]

The implementation of GISRA was a significant step in improving federal agencies' information security programs and initiating governmentwide actions. In addition, we believe that the recent enactment of legislation to continue such important information security requirements is essential to sustaining agency efforts to identify and correct significant weaknesses. Further, this new legislation reinforces the federal government's commitment to establishing information security as an integral part of its operations and helps to ensure that the administration and the Congress continue to receive the information they need to effectively manage and oversee federal information security.

Further information security improvement efforts are also needed at the governmentwide level. It is important that these efforts be guided by a comprehensive strategy and, as development of this strategy continues, that certain key issues be addressed.

First, the federal strategy should delineate the roles and responsibilities of the numerous entities involved in federal information security and describe how the activities of these organizations interrelate, who should be held accountable for their success or failure, and whether these activities will effectively and efficiently support national goals.

[13]U.S. General Accounting Office, *Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[14]U.S. General Accounting Office, *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD-00-33 (Washington, D.C.: November 1999).

[15]National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards and Technology*, Special Publication 800-30, January 2002.

Second, more specific guidance to agencies on the controls that they need to implement could help ensure adequate protection. Currently, agencies have wide discretion in deciding which computer security controls to implement and the level of rigor with which to enforce these controls. In essence, one set of specific controls will not be appropriate for all types of systems and data. Nevertheless, our studies of best practices at leading organizations have shown that more specific guidance is important.[16] 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. As discussed previously, the recently enacted Federal Information Security Management Act of 2002 requires NIST to develop standards that provide mandatory minimum information security requirements.

Third, ensuring effective implementation of agency information security and critical infrastructure protection plans will require active monitoring by the agencies to determine whether milestones are being met and testing to determine whether policies and controls are operating as intended. With routine periodic evaluations, such as those required by GISRA and now by the Federal Information Management Act of 2002, performance measurements would be more meaningful. In addition, the annual evaluation, reporting, and monitoring process established through these provisions is an important mechanism, previously missing, to hold agencies accountable for implementing effective security and to manage the problem from a governmentwide perspective.

Fourth, the Congress and the executive branch can use audit results to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by OMB and congressional efforts to oversee the Year 2000 computer challenge.

Fifth, agencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. As highlighted during the Year

[16]GAO/AIMD-98-68.

2000 challenge, the availability of adequate technical and audit expertise is a continuing concern to agencies.

Sixth, agencies can allocate resources sufficient to support their information security and infrastructure protection activities. In our review of first-year GISRA implementation, we reported that many agencies emphasized the need for adequate funding to implement security requirements, and that security funding varied widely across the agencies. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, additional amounts are likely to be needed to address specific weaknesses and new tasks. At the same time, OMB and congressional oversight of future spending on information security will be important for ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk-management process. Further, we agree with OMB that much can be done to cost-effectively address common weaknesses, such as limited security training, across government rather than individually by agency.

Seventh, expanded research is needed in the area of information systems protection. Although a number of research efforts are under way, experts have noted that more is needed to achieve significant advances. Further, in its December 2001 report, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (known as the "Gilmore Commission") recommended that the Office of Homeland Security develop and implement a comprehensive plan for research, development, testing, and evaluation to enhance cyber security.[17] In this regard, the Congress recently passed and the President signed into law the Cyber Security Research and Development Act to provide $903 million over 5 years for cybersecurity research and education programs.[18] This law directs the National Science Foundation to create new cybersecurity research centers, program grants, and fellowships. It also directs NIST to create new program grants for partnerships between academia and industry.

[17]*Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Dec. 15, 2001).

[18]P.L. 107-305, November 27, 2002.

Critical Infrastructure Protection Has Been Evolving Since the Mid-1990s, and Important Actions Have Taken Place

Over the years, a variety of working groups have been formed, special reports written, federal policies issued, and organizations created to address the nation's critical infrastructure challenges. In October 1997, the President's Commission on Critical Infrastructure Protection issued its report,[19] which described the potentially devastating implications of poor information security for the nation. In 1998, the President issued PDD 63, which 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 designated and established organizations to provide central coordination and support. This directive has since been supplemented by Executive Order 13231, which established the President's Critical Infrastructure Protection Board, and by the President's *National Strategy for Homeland Security.*[20]

Since 1998, a number of significant actions have taken place to better position the nation to protect our critical infrastructures.

- Several federal agencies have been designated to provide central coordination and support. For example, the Critical Infrastructure Assurance Office (CIAO), an interagency office housed in the Department of Commerce, was established to develop a national plan for critical infrastructure protection (CIP) on the basis of infrastructure plans developed by the private sector and federal agencies and to provide outreach to the private sector. In addition, the FBI's NIPC was expanded to (1) address national-level threat assessment, warning, vulnerability, and law enforcement investigation/response and (2) work with the private-sector-led information sharing and analysis centers (ISAC) that PDD 63 encouraged be created for infrastructure sectors to serve as mechanisms for gathering, analyzing, and disseminating threat, vulnerability, and incident information between the private sector and the federal government.

[19]*Critical Foundations: Protecting America's Infrastructures*, Report of the President's Commission on Critical Infrastructure Protection (October 1997).

[20]Office of Homeland Security, the White House, *National Strategy for Homeland Security*, July 2002.

- Partially in response to the events of September 11, 2001, in October of that year, the President established the President's Critical Infrastructure Protection Board to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures.[21] Chaired by the Special Advisor to the President for Cyberspace Security, the board has 10 standing committees to support its work on a wide range of critical information infrastructure efforts, including a committee for executive branch information systems security chaired by an OMB designee. The board is also intended to coordinate with the Office of Homeland Security, also created by the President in October 2001, with duties that include coordinating efforts to protect critical public and private information systems within the United States from terrorist attack.[22]

- In July 2002, the President and his Office of Homeland Security issued its *National Strategy for Homeland Security*, with strategic objectives to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. To ensure coverage of critical infrastructure sectors, this strategy identified 14 industry sectors, expanded from the 8 identified in PDD 63, as essential to our national security, national economic security, and/or national public health and safety. Lead federal agencies, known as sector liaisons, are to work with their counterparts in the private sector, known as sector coordinators, to assess sector vulnerabilities and to develop plans to eliminate vulnerabilities. The lead agencies for these sectors are listed in table 1.

[21]"Critical Infrastructure Protection in the Information Age," Executive Order 13231, October 16, 2001.

[22]"Establishing the Office of Homeland Security and the Homeland Security Council," Executive Order 13228, October 8, 2001.

Table 1: Critical Infrastructure Lead Agencies

Lead agency	Sectors
Department of Homeland Security	• Information and telecommunications • Transportation (aviation; rail; mass transit; waterborne commerce; pipelines; and highways, including trucking and intelligent transportation systems) • Postal and shipping • Emergency services • Continuity of government
Treasury	• Banking and finance
Health and Human Services	• Public health (including prevention, surveillance, laboratory services, and personal health services) • Food (all except for meat and poultry)
Energy	• Energy (electrical power, oil and gas production, and storage)
Environmental Protection Agency	• Water • Chemical industry and hazardous materials
Agriculture	• Agriculture • Food (meat and poultry)
Defense	• Defense industrial base

Source: *National Strategy for Homeland Security* and PDD63..

- NIPC currently reports that 12 ISACs have been established within the 14 sectors, including those for the chemical industry, surface transportation, electric power, telecommunications, information technology, financial services, water supply, oil and gas, emergency fire services, food, and emergency law enforcement. Additionally, NIPC has signed information-sharing agreements with most of these ISACs.

- The *National Strategy for Homeland Security* calls for the Office of Homeland Security and the President's Critical Infrastructure Protection Board to complete cyber and physical infrastructure protection plans, which would serve as the baseline for later development of a comprehensive national infrastructure protection plan. While the national strategy does not indicate a date when the comprehensive plan is to be completed, in September 2002, the board released a comment draft of a *National Strategy to Secure Cyberspace*.[23] Defined as steps the United States will take to secure the information technology networks necessary for the nation's economy, defense, and critical

[23]The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace—For Comment Draft*, September 2002.

services to operate, the strategy is divided into five audience levels, ranging from home users and small businesses to discussion of global issues. Level 3 describes the issues and challenges of, and makes recommendations for, critical sectors, including the federal government, state and local government, higher education, and the private sector.

- On November 25, 2002, the President signed the Homeland Security Act of 2002, which established the Department of Homeland Security. Regarding CIP, the new department is responsible for, among other things, (1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States; (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; and (3) disseminating, as appropriate, information analyzed by the department within the department and to other federal agencies, state and local government agencies, and private sector entities to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks. The act also transfers the functions, personnel, assets, and liabilities of NIPC (other than the Computer Investigations and Operations Section) and CIAO to the new department. This consolidation of essential CIP functions and organizations in the Department of Homeland Security may, if properly organized and implemented, lead over time to more efficient, effective, and coordinated programs.

Further Actions Needed to Improve CIP

Although the actions taken to date are major steps to more effectively protect our nation's critical infrastructures, we have identified and made numerous recommendations over the last several years concerning CIP challenges that still need to be addressed. For each of these challenges, improvements have been made and continuing efforts are in progress. However, much more is needed to address them. Further, it will also be important that CIP efforts are appropriately integrated with the implementation of the Department of Homeland Security. These challenges include the following:

- *Developing a national CIP strategy*: We have recommended that a more complete strategy is needed that will address specific roles, responsibilities, and relationships for all CIP entities; clearly define interim objectives and milestones; set time frames for achieving objectives; establish performance measures; and include all relevant sectors. In July 2002, we issued a report that highlights the importance of coordinating the many entities involved in cyber CIP efforts.[24] The recently issued draft *National Strategy to Secure Cyberspace* reiterates the importance of the sectors identified in PDD 63 and identifies additional sectors, but does not define the key federal agencies' roles and responsibilities associated with each of the sectors, nor does it define the relationships among the key CIP organizations. Until a comprehensive and coordinated strategy is completed that identifies roles and responsibilities for all CIP efforts, our nation risks not having a consistent and appropriate structure to deal with the growing threat of computer-based attacks on its critical infrastructure.

- *Improving analysis and warning capabilities:* More robust analysis and warning capabilities, including an effective methodology for strategic analysis and a framework for collecting needed threat and vulnerability information, are still needed to identify threats and provide timely warnings. Such capabilities need to address both cyber and physical threats. In April 2001, we reported on NIPC's progress in developing national capabilities for analyzing threat and vulnerability data, issuing warnings, and responding to attacks, among other issues.[25] Overall, we found that while progress in developing these capabilities was mixed, NIPC had initiated a variety of CIP efforts that had laid a foundation for future governmentwide efforts. In addition, NIPC had provided valuable support and coordination related to investigating and otherwise responding to attacks on computers. However, at the close of our review, the analytical capabilities that PDD 63 asserted were needed to protect the nation's critical infrastructures had not yet been achieved, and NIPC had developed only limited warning capabilities. In our report, we recognized that the administration was reviewing the government's

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

[25]U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 (Washington, D.C.: Apr. 25, 2001).

infrastructure protection strategy and recommended that, as the administration proceeds, the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

- establish a capability for strategically analyzing computer-based threats, including developing a related methodology, acquiring staff expertise, and obtaining infrastructure data; and

- require the development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources.

In July 2002, NIPC's director told us that, in response to our report recommendations, NIPC had developed a plan with goals and objectives to improve its analysis and warning capabilities and had made considerable progress in this area. The plan establishes and describes performance measures both for its analysis and warning section and for other issues relating to staffing, training, investigations, outreach, and warning. In addition, the plan describes the resources needed to reach the specific goals and objectives for the analysis and warning section. The director also told us that the analysis and warning section had created two additional teams to bolster its analytical capabilities. However, the director acknowledged that our recommendations were not yet fully implemented and that, despite the accomplishments to date, much more had to be done to create the robust analysis and warning capabilities needed to adequately address cyberthreats.

- *Improving information sharing on threats and vulnerabilities*: Information sharing needs to be enhanced both within the government and between the federal government and the private sector and state and local governments. Despite progress establishing ISACs, more needs to be done. Not every sector has a fully established ISAC, those that do have varied participation, and the amount of information being shared between the federal government and private-sector organizations also varies. The draft *National Strategy to Secure Cyberspace* states that the ISACs face several challenges, including enhancing the amount, timeliness, and effectiveness of the information being shared.

The *National Strategy for Homeland Security* also identifies partnering with nonfederal entities as a major initiative and discusses the need to

integrate information sharing within the federal government and among federal, state, and local governments and private industry. The strategy also discusses the need to use available public policy tools, such as grants.

For additional information on information security issues, please contact Robert F. Dacey, at (202) 512-3317 or daceyr@gao.gov.

Related GAO Products

Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk. GAO-03-303T. Washington, D.C.: November 19, 2002.

VA Information Technology: Management Making Important Progress in Addressing Key Challenges. GAO-02-1054T. Washington, D.C.: September 26, 2002.

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

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

FDIC Information Security: Improvements Made But Weaknesses Remain. GAO-02-689. Washington, D.C.: July 15, 2002.

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

Information Security: Corps of Engineers Making Improvements, but Weaknesses Continue. GAO-02-589. Washington, D.C.: June 10, 2002.

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

Information Security: Comments on the Proposed Federal Information Security Management Act of 2002. GAO-02-677T. Washington, D.C.: May 2, 2002.

Information Security: Additional Actions Needed to Fully Implement Reform Legislation. GAO-02-407. Washington, D.C.: May 2, 2002.

Information Security: Subcommittee Post-Hearing Questions Concerning the Additional Actions Needed to Implement Reform Legislation. GAO-02-649R. Washington, D.C.: April 16, 2002.

Information Security: Additional Actions Needed to Implement Reform Legislation. GAO-02-470T. Washington, D.C.: March 6, 2002.

Financial Management Service: Significant Weaknesses in Computer Controls Continue. GAO-02-317. Washington, D.C.: January 31, 2002.

Federal Reserve Banks: Areas for Improvement in Computer Controls. GAO-02-266R. Washington, D.C.: December 10, 2001.

Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets. GAO-02-231T. Washington, D.C.: November 9, 2001.

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

Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately-Controlled Systems from Computer-Based Attacks. GAO-01-1168T. Washington, D.C.: September 26, 2001.

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

Bureau of the Public Debt: Areas for Improvement in Computer Controls. GAO-01-1131R. Washington, D.C.: September 13, 2001.

Critical Infrastructure Protection: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities. GAO-01-1132T. Washington, D.C.: September 12, 2001.

Education Information Security: Improvements Made but Control Weaknesses Remain. GAO-01-1067. Washington, D.C.: September 12, 2001.

Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures. GAO-01-1073T. Washington, D.C.: August 29, 2001.

Nuclear Security: DOE Needs to Improve Control Over Classified Information. GAO-01-806. Washington, D.C.: August 24, 2001.

Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk. GAO-01-751. Washington, D.C.: August 13, 2001.

Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk. GAO-01-1004T. Washington, D.C.: August 3, 2001.

Information Systems: Opportunities Exist to Strengthen SEC's Oversight of Capacity and Security. GAO-01-863. Washington, D.C.: July 25, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-1005T. Washington, D.C.: July 25, 2001.

Information Security: Weak Controls Place Interior's Financial and Other Data at Risk. GAO-01-615. Washington, D.C.: July 3, 2001.

Critical Infrastructure Protection: NIPC Faces Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-769T. Washington, D.C.: May 22, 2001.

Computer-Based Patient Records: Better Planning and Oversight by VA, DOD, and HHS Would Enhance Health Data Sharing. GAO-01-459. Washington, D.C.: April 30, 2001.

Internet Privacy: Implementation of Federal Guidance for Agency Use of "Cookies." GAO-01-424. Washington, D.C.: April 27, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities. GAO-01-323. Washington, D.C.: April 25, 2001.

Computer Security: Weaknesses Continue to Place Critical Federal Operations and Assets at Risk. GAO-01-600T. Washington, D.C.: April 5, 2001.

VA Information Technology: Important Initiatives Begun, yet Serious Vulnerabilities Persist. GAO-01-550T. Washington, D.C.: April 4, 2001.

Internal Revenue Service: 2001 Tax Filing Season, Systems Modernization, and Security of Electronic Filing. GAO-01-595T. Washington, D.C.: April 3, 2001.

Internal Revenue Service: Progress Continues but Serious Management Challenges Remain. GAO-01-562T. Washington, D.C.: April 2, 2001.

Information Security: Safeguarding of Data in Excessed Department of Energy Computers. GAO-01-469. Washington, D.C.: March 29, 2001.

U.S. Government Financial Statements: FY 2000 Reporting Underscores the Need to Accelerate Federal Financial Management Reform. GAO-01-570T. Washington, D.C.: March 30, 2001.

Information Security: Challenges to Improving DOD's Incident Response Capabilities. GAO-01-341. Washington, D.C.: March 29, 2001.

Information Security: Progress and Challenges to an Effective Defense-Wide Information Assurance Program. GAO-01-307. Washington, D.C.: March 30, 2001.

Information Security: IRS Electronic Filing Systems. GAO-01-306. Washington, D.C.: February 16, 2001.

Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology. GAO-01-277. Washington, D.C.: February 26, 2001.

Information Security: Weak Controls Place D.C. Highway Trust Fund and Other Data at Risk. GAO-01-155. Washington, D.C.: January 31, 2001.

Performance and Accountability and High-Risk Series

Major Management Challenges and Program Risks: A Governmentwide Perspective. GAO-03-95.

Major Management Challenges and Program Risks: Department of Agriculture. GAO-03-96.

Major Management Challenges and Program Risks: Department of Commerce. GAO-03-97.

Major Management Challenges and Program Risks: Department of Defense. GAO-03-98.

Major Management Challenges and Program Risks: Department of Education. GAO-03-99.

Major Management Challenges and Program Risks: Department of Energy. GAO-03-100.

Major Management Challenges and Program Risks: Department of Health and Human Services. GAO-03-101.

Major Management Challenges and Program Risks: Department of Homeland Security. GAO-03-102.

Major Management Challenges and Program Risks: Department of Housing and Urban Development. GAO-03-103.

Major Management Challenges and Program Risks: Department of the Interior. GAO-03-104.

Major Management Challenges and Program Risks: Department of Justice. GAO-03-105.

Major Management Challenges and Program Risks: Department of Labor. GAO-03-106.

Major Management Challenges and Program Risks: Department of State. GAO-03-107.

Major Management Challenges and Program Risks: Department of Transportation. GAO-03-108.

Major Management Challenges and Program Risks: Department of the Treasury. GAO-03-109.

Major Management Challenges and Program Risks: Department of Veterans Affairs. GAO-03-110.

Major Management Challenges and Program Risks: U.S. Agency for International Development. GAO-03-111.

Major Management Challenges and Program Risks: Environmental Protection Agency. GAO-03-112.

Major Management Challenges and Program Risks: Federal Emergency Management Agency. GAO-03-113.

Major Management Challenges and Program Risks: National Aeronautics and Space Administration. GAO-03-114.

Major Management Challenges and Program Risks: Office of Personnel Management. GAO-03-115.

Major Management Challenges and Program Risks: Small Business Administration. GAO-03-116.

Major Management Challenges and Program Risks: Social Security Administration. GAO-03-117.

Major Management Challenges and Program Risks: U.S. Postal Service. GAO-03-118.

High-Risk Series: An Update. GAO-03-119.

High-Risk Series: Strategic Human Capital Management. GAO-03-120.

High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures. GAO-03-121.

High-Risk Series: Federal Real Property. GAO-03-122.

GAO's Mission

The General Accounting Office, the 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 GAO Mailing Lists" under "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

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00