United States General Accounting Office

GAO

Report to the Ranking Minority Member, Subcommittee on 21st Century Competitiveness, Committee on Education and the Workforce, House of Representatives

September 2002

EMPLOYEE PRIVACY

Computer-Use Monitoring Practices and Policies of Selected Companies

GAO-02-717

Contents

Tables

Abbreviations

ECPA Electronic Communications Privacy Act of 1986

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

September 27, 2002

The Honorable Patsy T. Mink
Ranking Minority Member
Subcommittee on 21st Century
Competitiveness
Committee on Education
and the Workforce
House of Representatives

Dear Ms. Mink:

Over the past decade, there has been a technological revolution in the workplace as businesses have increasingly turned to computer technology as the primary tool to communicate, conduct research, and store information. As the use of computer technology has increased, so has concern grown among private sector employers that their computer resources may be abused by employees—either by accessing offensive material or jeopardizing the security of proprietary information—and may provide an easy entry point into a company's electronic systems by computer trespassers. As a result, companies have developed "computer conduct" policies and implemented strategies to monitor their employees' use of e-mail, the Internet, and computer files. National surveys have reported that many companies are engaged in such practices. Federal and state laws and judicial decisions have generally given private sector companies wide discretion in their monitoring and review of employee computer transmissions, including the Internet and e-mail. However, some legal experts believe that these laws should be more protective of employee privacy by limiting what aspects of employee computer use employers may monitor and how they may do so.

Private sector practice of monitoring their employees' electronic transactions has raised questions about the appropriate balance between employees' privacy rights in the workplace and companies' rights to protect themselves and their employees by monitoring their employees' electronic transactions. In addition, following the September 11, 2001, terrorist attacks on the United States, policymakers re-examined many

similar privacy issues as they debated the USA PATRIOT Act,[1] which expands the federal government's authority to monitor electronic communications and Internet activities. You asked us to determine from a diverse group of private sector companies (1) to what extent and for what purpose selected private sector employers gather information on employees' use of e-mail, the Internet, and computer files; (2) to what extent these private sector employers notify their employees of their policies on the use and review of e-mail, the Internet, and computer files; and (3) whether these private sector employers have changed their policies and practices on gathering information on employees' use of computer resources as a result of the September terrorist attacks.

To gather information to respond to these questions, we reviewed the literature and research on private and public sector monitoring of employees' use of e-mail, the Internet, and computer files. In addition, we interviewed privacy experts from universities, officials and researchers from national business organizations, and officials from the Department of Labor and the National Labor Relations Board.[2] To illustrate private sector policies and practices regarding monitoring, we conducted interviews with officials from 14 Fortune 1,000 private sector companies from five industry categories—financial services, general services, manufacturing, professional services, and wholesale/retail. Eight of the interviews were by telephone and 6 were site visits. In these discussions, we talked with various company officials, including representatives from their general counsel's offices, human resource departments, internal audit, and computer security administrators. The data gathered from these 14 companies are for illustrative purposes only and do not represent the monitoring policies and procedures for all private sector companies in the United States. We obtained detailed information on written policies covering the employee use of company computer resources and reviewed the written policies of 8 of these companies. We also obtained comments on a draft of this report from experts on employee rights and the legal aspects of private sector monitoring. Because there are no federal executive agencies with oversight responsibilities in this area, we did not obtain federal agency comments on this report. We conducted our work

[1]Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, P.L. 107-56, October 26, 2001.

[2]The National Labor Relations Board is an independent federal agency, and one of its principle functions is to prevent and remedy unfair labor practices by either labor unions or private sector employers.

between September 2001 and August 2002 in accordance with generally accepted government auditing standards.

Results in Brief

All 14 companies we reviewed store their employees' electronic transactions: e-mail messages, information of Internet sites visited, and computer file activity. These companies reported they collect this information to create duplicate or back-up files in case of system disruptions; to manage computer resources such as system capacity to handle routine e-mail and Internet traffic; and to hold employees accountable for company policies. Eight of these companies reported that they would read and review these electronic transactions if they receive other information that an individual may have violated company policies. When such circumstances arise, these employers can review employees' electronic transactions to find if violations of company computer-use policies such as visits to sites containing offensive or disruptive material and improper protection of proprietary information have occurred. On the other hand, 6 companies we contacted routinely analyzed their employees' transactions to find possible inappropriate uses of company computer resources. While all the companies we contacted have investigated employees for misuse of computer resources, company officials told us that such investigations are rare and, if violations of company policies are found, result in a range of disciplinary actions.

Representatives from all of the companies we contacted had policies that contained most of the elements experts agreed should be included in company computer-use policies. For example, all company policies affirmed their rights to review employee use of company computer assets, described appropriate employee uses of these assets, and detailed penalties for misuse. We also found that all companies disseminated information about these policies, although in a variety of ways. For example, 8 companies require new employees to attend training that includes the review of companies' computer-use policies. Some companies required employees to complete on-line training while others used videotapes. Another company we reviewed conducted biannual sessions on appropriate business conduct, which included appropriate e-mail and Internet behavior.

We found that none of the companies we studied had changed any of their employee computer-use policies or monitoring practices after the September 11 terrorist attacks. Most companies did, however, report a growing concern about electronic intrusion into their computer systems from outside trespassers or viruses and had increased their vigilance by

strengthening their surveillance of incoming electronic transmissions. Most companies had, for instance, begun to delete certain attachments from incoming e-mail, and some block incoming e-mails based on certain words or phrases in the subject line or text. This apprehensiveness concerning possible threats did not lead company officials to increase either their suspicion of employees or the information they collected from them. But new vigilance against demonstrated dangers and nuisance is leading companies to tighten control over their computer systems.

Background

For more than a decade, rapid increases in the use of computer technology, both at work and in the home, have changed the way Americans work and communicate. As of September 2001, 174 million people—66 percent of the U.S. population—were using computers in their homes, schools, libraries, and work. In the workplace, 65 million of the 115 million employed adults age 25 and over, almost 57 percent, used a computer at work. However, in recent years, while the increase in the percentage of employees using computers has been modest (52 percent in 1998 to 57 percent in 2001), the percentage using the Internet and/or e-mail at work grew from about 18 percent in 1998 to almost 42 percent in 2001.[3]

As the use of these electronic technologies has increased in the workplace, so have employers' concerns about their employees' use of company-owned computing systems—e-mail, the Internet, and computer files—for activities other than company business. Likewise, privacy advocates have raised concerns about the potential for employers to infringe upon employees' right to privacy. In response to these concerns, many employers have developed policies to notify their employees that they monitor use of these systems and to provide guidance to employees about the appropriate uses of the computing technologies. Information on the number of private sector companies that monitor their employees, their monitoring practices, and their effects on employee productivity and morale is very limited. While some of these studies suffer from methodological limitations such as low response rates, taken together they seem to indicate a general trend towards employers' increased monitoring

[3]U.S. Department of Commerce, *A Nation Online: How Americans Are Expanding Their Use of the Internet*, February 2002.

of their employees.[4] In addition, software developers have made it easier and inexpensive for businesses to monitor their employees by creating software that can, for example, scan e-mail messages for certain words or phrases and/or block inappropriate Internet sites.

Current Law Allows Wide Discretion in Employer Monitoring

The Electronic Communications Privacy Act (ECPA) of 1986,[5] which is intended to provide individuals with some privacy protection in their electronic communications, has several exceptions that limit its ability to provide protection in the workplace. For example, the act does not prevent access to electronic communications by system providers, which could include employers who provide the necessary electronic equipment or network to their employees. (See, e.g., U.S. v. McLaren, 957 F. Supp. 215 (M.D. Fla. 1997)). Because the ECPA provides only limited protection to private sector employees, some privacy advocates have called for a new law that would specifically address workplace computer privacy and limit the powers and means of employer monitoring. The most recent federal statute affecting privacy in the workplace is the USA PATRIOT Act,[6] which was enacted in the wake of the September 11, 2001, terrorist attacks. This act expands the federal government's authority to monitor electronic communications and Internet activities, including e-mail. However, no federal executive agency has general oversight responsibilities for private sector employee-monitoring programs.

Many states have statutes that are similar to the ECPA, with greater protection in some cases. Additional protection may be provided through state common law, which is based on judicial precedent rather than legislative enactments. Such decisions, however, have generally given employers substantial leeway in monitoring computer use of their employees. While state common law may recognize the right of an individual to take legal action for an offense known generally as "invasion of privacy," such actions historically have not provided employees with additional protections. Courts have found that employers' monitoring of their employees' electronic transmissions involving e-mail, the Internet,

[4]American Management Association, *2001 AMA Survey Workplace Monitoring & Surveillance Summary of Key Findings;* The Society for Human Resource Management, *2000 Workplace Privacy Survey;* The Privacy Foundation, *The Extent of Systematic Monitoring of Employee E-mail and Internet Use,* July 2000.

[5]P.L. No. 99-508.

[6]P.L. No. 107-56.

and computer file usage on company-owned equipment is not an invasion of privacy. Invasion of privacy claims against an employer generally require employees to demonstrate, among other things, that they had a "reasonable expectation of privacy" in their communications. Courts have consistently held, however, that privacy rights in such communications do not extend to employees using company-owned computer systems, even in situations where employees have password-protected accounts.

Private Sector Companies Gathered Information on Employees' Computer Use and Some Read and Reviewed Contents

All 14 companies we contacted routinely collected and stored employee e-mail messages, information on Internet sites visited, and computer file activity. Eight of these companies reported that they only read or reviewed information on employees' electronic transmissions once the company determined that a further investigation of employee conduct was warranted. However, 6 of 14 companies told us that they routinely performed additional analyses on the stored information to determine if employees were misusing company computer resources. For example, these companies routinely searched the e-mail message titles, addresses, or contents for proprietary information or offensive language. In general, we found that the companies we studied initiated few investigations of employee computer conduct. Most of the companies that have reviewed information on employees' electronic transmissions and determined that misuse occurred, reported that penalties ranged from counseling and warnings to termination.

Companies Routinely Collected and Stored Information on Employee E-mail, the Internet, and Computer Files

All 14 companies collected and retained electronic transmission data as part of their normal business operations, primarily as backup files and to manage their computer resources. Backup files can be quickly restored if a computer system failure occurs, and the company's operations can continue with as little interruption as possible. However, according to company officials, the information on these backup files was also available as a source of data for reviews of individual employee e-mail messages, Internet use, or computer files. Company officials also said that stored data were used to manage their computer resources. For example, officials at one company told us that they collect e-mail and Internet data to track the systems' capacity. Another company's representatives said they use the collected information for troubleshooting and to correct network problems.

The 14 companies collected different information for e-mail, Internet use, and computer files. For e-mail messages, officials from the 14 companies reported they generally collect and store all business and personal

incoming and outgoing e-mail messages including attachments, addresses, and the date and time the e-mail was sent or received. For the Internet sites visited, generally the information collected included the web address and the date and time the website was used. For computer file activity, all the contents of the files on their network computer systems were backed-up daily. Officials from the 14 companies reported they retained these data for short periods of time. Nine of these companies said that they generally retained these files for 90 days or less, and one company kept its e-mail data for as little as 3 days.

Certain Companies Read and Reviewed Employee Computer Use Information Only as a Part of an Investigation

Eight of the companies reported that they would only review the employee electronic transmission data they collected if there was an indication of employee misuse of computer resources and the company initiated an investigation. Generally, investigations were initiated by either a complaint submitted to management by a company employee or a "request for information" by management concerning an employee's conduct. These initiating requests were usually reviewed by a number of company officials, including representatives from Human Resources, General Counsel, or Computer Security prior to the actual retrieval of employee information. Company officials told us that unless they received a request for data, they would not review any of their employees' electronic transmissions. They added that access to any data collected for an investigation is restricted to a limited number of company officials. Company officials cited several reasons for establishing this reactive approach for reviewing employee electronic transmissions. One company believed it was important to establish an atmosphere of trust and presumed employees would use the system primarily for business purposes. Another company's officials said that they did not have enough resources to actively monitor their employees' electronic transmissions.

Other Companies Routinely Reviewed Selected E-mail and/or Internet Data for Inappropriate Use

Six of the 14 companies we contacted, in addition to collecting and storing information on employee computer use, performed routine analyses on all employee e-mail or Internet data resulting in the review of selected electronic transmissions. These companies reviewed the electronic transmission information for several reasons. Company officials reported that they needed to protect proprietary information and prevent Internet visits to inappropriate sites. For example, 3 companies reviewed e-mail messages using commercial software that searched for keywords. These companies selected the words to be searched, and a computer file of e-mail messages that matched pre-selected key words would be

generated. Company officials routinely reviewed this file to determine if e-mails contained inappropriate material.

Other companies reported different strategies to identify employee misuse of computer resources. One company's computer security office generated a weekly report of the 20 employees who logged on the Internet the most times and listed the sites visited. Officials reviewed this list to determine if inappropriate sites have been visited. A second company reviewed the Internet use of a random sample of 10 to 20 employees each month. This review was intended to identify employees who had visited offensive or inappropriate sites. Employees identified through this process were generally counseled against further misuse. Finally, one company, in 2001, monitored the inappropriate websites employees visited, such as hate, violence, and pornographic, and in 2002, it purchased new software to block these offensive sites.[7]

All Companies Had Few Investigations and Disciplinary Actions for Inappropriate Use of E-mail, the Internet, and Computer Use

Generally, the companies we reviewed—regardless of whether they routinely reviewed employee computer use or examined individual employee records only to pursue particular complaints—reported that the total number of investigations was very small as a proportion of the number of employees with access to e-mail, the Internet, or computer files.[8] The number of annual investigations ranged from 5 to 137 and represented less than 1 percent of the total domestic employees at these companies. For example, one company with more than 50,000 domestic employees reported 72 e-mail investigations and 48 Internet investigations in calendar year 2001.

We found companies most often investigated the alleged misuse of employee e-mail followed by investigations of Internet use. Not surprisingly, the company that routinely reviewed employee Internet use initiated the most investigations on employee Internet conduct—90 investigations. Investigations of the content of employees' computer

[7]At the time of our review, 8 of the 14 companies had computer software that would block entry into predetermined Internet sites. However, 2 more companies installed blocking software in calendar year 2002.

[8]Six of the 14 companies we reviewed could report separately on investigations that centered on inappropriate computer use. The remaining companies could not report employee investigation by specific categories of alleged offenses.

files were the smallest in number, and only one company told us that they had initiated investigations related to them.

Only 2 of the 14 companies we interviewed were able to provide data on the types of disciplinary actions taken against employee misuse of computer resources. One company reported that of its 20,000 employees, it terminated 2 employees for inappropriate e-mail use, 2 for Internet misuse, and 1 for computer file violation in 2001. The other company reported that over a 5-year period it had terminated 14 employees for misuse of the Internet. Most of the 14 companies reported various types of actions that could be taken against employees for inappropriate use of computer resources. Four companies told us these actions ranged from informal discussions or formal counseling between the employee and company managers to terminations. Only the most flagrant and repeated violations would result in employee termination.

Companies Developed Computer-Use Policies and Informed Their Employees

The 14 companies we reviewed all have written policies that included most of the elements recommended in the literature and by experts as critical to a company computer-use policy. There is a general consensus that policies should at least affirm the employer's right to review employee use of company computer assets, explain how these computer assets should and should not be used, and forewarn employees of penalties for misuse. We also found that all companies disseminated information about these policies through their company handbooks, and 8 discussed their computer-use policies with new employees at the time of hire. In addition, some companies provided annual training to employees on company policies, and others sent employees periodic reminders on appropriate computer conduct.

Companies Generally Included Critical Elements in Their Computer-Use Policy

The 14 companies we reviewed had written policies that explained employee responsibilities and company rights regarding the use of company-owned systems. Our discussions with company officials and review of written policies showed that all 14 contain most, if not all, of the policy elements recommended by experts. From our review of the literature and discussions with legal experts, privacy advocates, and business consultants, we identified common elements that should be included in company computer-use policies (see table 1).[9] These experts

[9]For examples, see *Internet Acceptable-Use Policies*, National Legal Research Group, Inc., 2000.; Nancy Flynn, *The ePolicy Handbook*. AMA Publications, 2001.

generally believed that the most important part of a company's computer-use policy is to inform employees that the tools and information created and accessed from a company's computer system are the property of the company and that employees should have no "expectation of privacy" on their employers' systems. Courts have consistently upheld companies' monitoring practices where the company has a stated policy that employees have no expectation of privacy on company computer systems. The experts also agreed computer-use policies should achieve other company goals, such as stopping release of sensitive information, prohibiting copyright infringement, and making due effort to ensure that employees do not use company computers to create a hostile work environment for others. Finally, according to experts, employees should clearly understand the consequences for violating company computer policies. For example, one company's computer-use policy states that "violators [of company Internet/Intranet use policy] are subject to disciplinary action up to termination of employment and legal action."

Table 1: Key Elements of a Computer-Use Policy

Policy element	Type of statement
Monitoring use of proprietary assets	Statements that company computing systems are provided as tools for business and all information created, accessed, or stored using these systems are the property of the company and subject to monitoring, auditing, or review.
Establishing no expectation of privacy	Statements about the extent or limitations of privacy protections for employee use of e-mail, the Internet, and computer files.
Improper employee use	Statements that some uses of company computers are inappropriate - including specific notice banning offensive material (e.g., obscenity, sexual content, racial slurs, derogation of people's personal characteristics), and language relating e-mail and Internet use to general prohibitions of harassment.
Allowable employee uses	Statements explaining proper or acceptable uses of the company systems, including whether or not personal use is permitted.
Protecting sensitive company information	Statements providing instructions for handling proprietary information on company systems.
Disciplinary action	Statements that there are penalties and disciplinary actions for violations of company usage policy.
Employee acknowledgement of policy	A statement requiring that employees demonstrate they understand the company policy and acknowledge their responsibility to adhere to the policy.

Source: GAO's analysis of recommended computer-use policies.

While the experts we interviewed recommended that employers include the above elements so that employees can be informed and acknowledge that they have no expectation of privacy on company-owned systems, some experts recommended additional steps that would help to protect employee privacy. For example, one expert recommended that employee groups participate in the formulation and review of monitoring policies; and another expert recommended that employees have access to any

information collected on their electronic transmissions. Furthermore, other experts recommended an alternate policy framework that would preclude employers' review of employee electronic transmissions except when they have a reasonable independent indication of inappropriate use.

From our review of company computer-use policies, including interviews with private sector officials and reviews of written policies, we determined that all 14 companies generally addressed most of the seven key elements of a computer-use policy (see table 2).

Table 2: Company Notification Practices

	Employer policies of 14 companies		
Key elements of computer-use policy	**Specifically addressed**	**Generally addressed**	**Not addressed**
1. Monitoring use of proprietary assets	9	5	0
2. Establishing no expectation of privacy	7	7	0
3. Improper employee use	7[a]	7	0
4. Allowable employee uses	14	0	0
5. Protecting sensitive company information	14	0	0
6. Disciplinary action	14	0	0
7. Employee acknowledgement of policy	12	0	2

[a]Seven companies specifically identified harassment as an improper use of their computers.

Source: Company interviews and computer-use policies.

While we determined that these 14 companies' computer-use policies generally addressed the key elements,[10] we found that there was variation in the specificity in policy statements. For example, one company's policy statement regarding "Monitoring Use of Proprietary Assets" stated, "[company] reserves the right to access and monitor the contents of any system resource utilized at its facilities." Another company's policy stated, "the information and communications processed through your account are subject to review, monitoring, and recording at any time without notice or permission." An official from another company, which only collected and stored employee computer use information and did not routinely review electronic transmissions, told us his company informed employees of its capacity to monitor its property with the more general statement that "data is collected and the company reserves the right to review this data." Only one company reported that its policy did not include language

[10]We obtained and reviewed from eight companies the written policies that covered the employees' use of company computer resources. The other six companies declined to provide us with their written policies but were willing to discuss them.

specifically informing employees that their computer use was subject to review by other people in the company. Representatives from this company told us that their policy does, however, include a statement that employee messages could be accessed and that the company could not ensure their confidentiality.

Under "Establishing No Expectation of Privacy" some companies directly inform employees that they should under no circumstances expect privacy. For example, one policy stated, "All users should understand that there is no right or reasonable expectation of privacy in any e-mail messages on the company's system." Somewhat less explicit, another policy stated, "Our personal privacy is not protected on these systems, and we shouldn't expect it to be." Some companies generally implied the principle of "no expectation of privacy" with statements like, "[company] reserves the right to audit, access, and inspect electronic communications and data stored or transmitted on its Computer Resources."

Finally, the employers we reviewed also addressed improper uses of computer resources. All company representatives had policies that notified employees about improper uses; and the eight written policies we reviewed contained specific prohibitions on the use of company resources to create or transmit offensive material. Moreover, seven of these policies included some form of the word "harass" under their discussion of prohibited or inappropriate uses of corporate systems, and some also included a form of the word "discriminate." No two policies addressed this issue in exactly the same terms, but representative statements prohibited behaviors such as "viewing or communicating materials of an obscene, hateful, discriminatory or harassing nature"; "any messages or data that…defames, abuses, harasses or violates the legal rights of others"; and "Accessing, downloading, or posting material that is inappropriate, fraudulent, harassing, embarrassing, profane, obscene, intimidating, defamatory, unethical, abusive, indecent or otherwise unlawful." Experts recommend that policies include such specific prohibitions in order to limit a company's liability for workplace lawsuits, and they stress the importance of ensuring that employees understand the company's definitions of inappropriate use.

Companies Informed Employees of Their Policies in a Variety of Ways

Both the literature we reviewed and experts we interviewed agreed that establishing company policies on employee computer use is incomplete without strategies to disseminate the information. Experts pointed out that informing employees about these policies not only established the limits of employee expectations about privacy but also allowed them the

opportunity to conform their behavior to the circumstances of having limited privacy. Among the 14 companies we contacted, we found multiple and active ways to inform and remind employees about the policies concerning the use of computer systems. Officials at 8 of the companies we reviewed said that at the time of hire, new employees receive training on company policies for using the computer systems. Officials from 5 companies told us they required all employees to participate in an annual review of their computer-use policies, either through an Intranet-based training or over e-mail. Other training techniques company officials described to us included business conduct reviews every 2 years, weekly e-mail reminders of their policies, and a series of videotapes that explain policies to employees. In addition to training programs, 10 companies have daily messages referring to the corporate policies that employees must acknowledge before they are allowed to log in to the systems.

Companies Have Not Changed Their Computer-Use Policies or Monitoring Practices as a Result of the September 11 Terrorist Attacks

None of the companies' representatives we interviewed said that they had changed any of their computer-use polices or practices as a result of the terrorist attacks on September 11, 2001. Officials from four companies reported that after September 11th, they had been asked by law enforcement agencies to provide information about their employees' and customers' use of their e-mail systems and other sources and that they had complied with these requests. But none of the employers we interviewed had increased the amount or type of information they gathered on employees' use of e-mail, the Internet, or computer files. However, representatives from 10 companies did report increased concern for the security of their computer systems from outside trespassers or viruses entering their systems through e-mail or from imported computer files. Seven company representatives mentioned the Code Red Worm—which appeared around July 2001—and the Nimda virus—entering computer networks on September 18, 2001—as particular examples of the most serious kind of threat they faced and said these events had motivated them to strengthen the virus protection of their systems. Ten of the companies we reviewed told us that they have procedures to screen incoming e-mail messages for viruses, for example, by deleting file attachments with an "exe" extension[11] from all incoming e-mail messages. In early 2002, one company began and another was preparing to use software that searches title lines of incoming e-mail and deletes messages with sex-themed

[11]Many viruses are contained in "exe" (executable) file attachments to e-mail messages and enter the computer system when the executable file is opened.

language, simply because the volume of unsolicited e-mail had begun to overwhelm their systems. Such actions reflect the widespread belief among the company officials we interviewed that the worst nuisance and most likely threat to company computer systems comes from outside trespassers with a capacity to paralyze a company's Internet infrastructure or disrupt business, rather than the company's own employees.

We are sending copies of this report to the Secretary of Labor and other interested parties. We will also make copies available to others upon request. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

Please contact me on (202) 512-7215 if you or your staff have any questions about this report. Key contributors to this report are listed in appendix I.

Sincerely yours,

Robert E. Robertson
Director, Education, Workforce
and Income Security Issues

Appendix I: GAO Contacts and Staff Acknowledgments

GAO Contacts

David D. Bellis, (415) 904-2272
Richard L. Harada, (206) 287-4841

Staff Acknowledgments

In addition to the individuals named above, Nancy R. Purvine, Eric A. Wenner, Shana Wallace, and Julian P. Klazkin made key contributions to this report.

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 daily E-mail alert for newly released products" under the GAO Reports 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