



GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 26, 2009

The Honorable Robert C. Byrd
Chairman
The Honorable George Voinovich
Ranking Member
Committee on Appropriations
Subcommittee on Homeland Security
United States Senate

The Honorable David E. Price
Chairman
The Honorable Harold Rogers
Ranking Member
Committee on Appropriations
Subcommittee on Homeland Security
House of Representatives

Subject: *The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report*

In 2005, Hurricane Katrina devastated the Gulf Coast, damaging critical infrastructure, such as oil platforms, pipelines, and refineries; water mains; electric power lines; and cellular phone towers. The infrastructure damage and resulting chaos disrupted government and business functions alike, producing cascading effects far beyond the physical location of the storm. Threats against critical infrastructure are not limited to natural disasters. For example, in 2005, suicide bombers struck London's public transportation system, disrupting the city's transportation and mobile telecommunications infrastructure. In March 2007, we reported that our nation's critical infrastructures and key resources (CIKR)—systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters—continue to be vulnerable to a wide variety of threats.¹ According to DHS, because the private sector owns approximately 85 percent of the nation's CIKR—banking and financial institutions, telecommunications networks, and energy

¹ GAO, *Critical Infrastructure: Sector Plans Complete and Sector Councils Evolving*, [GAO-07-1075T](#) (Washington, D.C.: July 12, 2007); and *National Cybersecurity Strategy: Key Improvements are Needed to Strengthen the Nation's Posture*, [GAO-09-432T](#) (Washington, D.C.: Mar. 10, 2009).

production and transmission facilities, among others—it is vital that the public and private sectors work together to protect these assets.

The Homeland Security Act of 2002 created DHS and gave the department wide-ranging responsibilities for, among other things, leading and coordinating the overall national critical infrastructure protection effort.² For example, the act required DHS to (1) develop a comprehensive national plan for securing the nation’s CIKR and (2) recommend measures to protect CIKR in coordination with other agencies of the federal government and in cooperation with state and local government agencies and authorities, the private sector, and other entities. Homeland Security Presidential Directive 7 (HSPD-7) further defined critical infrastructure protection responsibilities for DHS and those federal agencies—known as sector-specific agencies (SSA)—responsible for particular industry sectors, such as transportation, energy, and communications. HSPD-7 directed DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across CIKR sectors.³ Also, in accordance with the Homeland Security Act and in response to HSPD-7, DHS issued, in June 2006, the National Infrastructure Protection Plan (NIPP), which provides the overarching approach for integrating the nation’s many CIKR protection initiatives into a single national effort. The NIPP sets forth a comprehensive risk management framework and clearly defined roles and responsibilities for DHS, SSAs, and other federal, state, regional, local, tribal, territorial, and private sector partners implementing the NIPP.⁴ Within this framework DHS has emphasized the importance of collaboration and partnering with CIKR stakeholders, and relies on voluntary information sharing between the private sector and DHS to better protect and ensure the resiliency of CIKR in the United States.

The Conference Report accompanying the Department of Homeland Security Appropriations Act, 2005, directed DHS to complete an analysis on whether the department should require private sector entities to provide DHS with existing information about their security measures and vulnerabilities in order to improve the department’s ability to evaluate critical infrastructure protection nationwide.⁵ This direction was consistent with concerns raised by the House Appropriations Committee about DHS’s progress conducting vulnerability assessments for critical infrastructure facilities generally, and security measures at chemical facilities in particular. The analysis was to include all critical infrastructure, including chemical

² See generally Pub. L. No. 107-296, 116 Stat. 2135 (2002). Title II of the Homeland Security Act, as amended, primarily addresses the department’s responsibilities for critical infrastructure protection.

³ The 17 sectors identified pursuant to HSPD-7 are the agriculture and food sector; the banking and finance sector; the chemical sector; the commercial facilities sector; the commercial nuclear reactors, materials, and waste sector; the communications sector; the dams sector; the defense industrial base sector; the drinking water and water treatment systems sector; the emergency services sector; the energy sector; the government facilities sector; the information technology sector; the national monuments and icons sector; the postal and shipping sector; the public health and health care sector; and the transportation systems sector. DHS created the critical manufacturing sector as an 18th sector in 2008. Enclosure I discusses how the National Infrastructure Protection Plan (NIPP) provides the framework for organizing and managing risk to the U.S.’s CIKR and shows how the NIPP assigns responsibility for CIKR sectors to SSAs.

⁴ DHS issued a revised NIPP in 2009.

⁵ See H.R. Conf. Rep. No. 108-774, at 75-76 (Oct. 9, 2004) (accompanying H.R. 4567, the DHS Appropriations Bill, 2005, enacted as Public Law 108-334, 118 Stat. 1298 (2004)). The Conference Report did not specify a date for submission.

plants; the costs to the private sector for implementing such a requirement; the benefits of obtaining the information; and costs to DHS's Information Analysis and Infrastructure Protection (IAIP) (presently the Office of Infrastructure Protection (IP)) to implement this requirement.⁵ The Conference Report further directed us to review the quality of the analysis and report to the House and Senate Committees on Appropriations within 3 months after completion of the analysis. DHS provided us a copy of the report on February 23, 2009. According to DHS, the report was completed in 2005 and information was subsequently updated in June 2007.⁶ However, based on discussions with your staff and IP officials, the report was never delivered to the Senate and House Appropriation Committees. As agreed with your staff in March 2009, due to the age of DHS's report, this correspondence summarizes DHS's approach for preparing its report and documents the results of our efforts in order to fulfill our responsibility as directed in Conference Report 108-774.

To determine DHS's approach for preparing the report, we reviewed the cost-benefit report and met with DHS officials in IP to better understand how the report was prepared and why it was prepared in that manner. We also compared it to Office of Management and Budget (OMB) Circular A-4 which provides criteria federal agencies are to use when performing a regulatory analysis. Specifically, the circular, which is based on best practices, is designed to standardize the way benefits and costs of federal regulatory actions are measured and reported to (1) help learn if the benefits of a proposed action are likely to justify the costs, and (2) discover which of the possible alternatives is the most cost-effective. Among other things, the circular stipulates that the regulatory analysis include a quantitative analysis of costs and benefits.⁸ In unusual cases where there is no quantified information on either benefits or costs, the circular allows agencies to do a qualitative analysis and suggests that professional judgment be used to highlight those costs and benefits believed to be the most important. In either case, the circular calls for agencies to compare the benefits with the costs in the regulatory analysis.

We conducted this performance audit from February 2009 to June 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

⁵ As a result of a subsequent DHS reorganization, the applicable mission of the Under Secretary for IAIP now resides with the Under Secretary for National Protection and Programs. Although the Conference Report specifically directed IAIP to conduct this analysis, we have generalized this direction to the Department due to its subsequent reorganization.

⁶ Report to Congress: *Mandatory Information Sharing for the Protection of Critical Infrastructure and Key Resources: The Costs and Benefits of Requiring Information from the Private Sector on Security Measures and Vulnerabilities*, Department of Homeland Security, the Office of Infrastructure Protection (IP), Partnership and Outreach Division, (June 2007). This report has been designated For Official Use Only (FOUO).

⁸ According OMB Circular A-4, a quantitative analysis of costs and benefits would require that benefits and costs be expressed in monetary or physical units, if possible, so that the regulatory alternative that maximizes net benefits (the difference between benefits and costs) can be identified.

Results

DHS used two contractors to complete the cost-benefit report at a cost of about \$3.4 million.⁹ In August 2005, the first contractor developed a draft proposal that discussed the scope of the information required to complete the report and the security and vulnerability information currently available to DHS. It also proposed surveying the public and private sectors to collect information on the costs and benefits of providing vulnerability assessment and security information to DHS. DHS officials said that DHS rejected this approach because DHS was involved in developing a public-private partnership structure and officials believed that doing a survey on possible regulatory costs would have adversely affected the partnership building process. DHS officials also said that the Paperwork Reduction Act (PRA)—which requires agency requests for information to undergo internal and Office of Management and Budget review and approval and includes, among other requirements, public comment periods for the proposed information-gathering method¹⁰—could have resulted in some delays in gathering data for the report, but it was not the primary reason for rejecting the proposed survey approach.

DHS subsequently tasked the second contractor to complete the report using a different methodology, and according to DHS, this contractor produced a draft report in December 2005. This contractor compiled publicly available information on the costs and benefits to the public and private sectors of requiring vulnerability and security information be provided to DHS. Although the second contractor's report discussed potential public and private sector costs and benefits, it did not articulate which of these costs and benefits were most important, nor did it conclude whether the costs exceeded the benefits, or vice a versa, with regard to potential requirements for the private sector to provide information on vulnerabilities and existing security measures. Circular A-4 states that the objective of cost-benefit analysis is to produce a measure of the difference between benefits and costs and that when costs and benefits are based on a qualitative analysis, those deemed to be the most important are to be highlighted. DHS took receipt of the second contractor's report and, according to DHS officials, continued to revise it throughout the following year to incorporate information from the final NIPP and its supporting sector specific plans.¹¹ In addition to a discussion of potential costs and benefits, DHS's final report, dated June 2007, includes a general discussion of critical infrastructure risk management and associated information needs, an overview of the existing regulatory environment for each of the CIKR sectors, and the availability of security information and its utility to security partners, such as CIKR owners and operators.¹²

⁹ DHS officials told us that, based on available records, the first contractor, MITRE, received over \$558,000 and the second contractor, Energetics, received more than \$2.8 million for work related to the cost-benefit report.

¹⁰ The purpose of the Paperwork Reduction Act, among other things, is to minimize the paperwork burden for individuals, small businesses, and educational and nonprofit institutions, federal contractors, and state, local and tribal governments, and other persons resulting from the collection of information by or for the federal government. See 31 U.S.C. § 3501. For a more complete discussion, see GAO, *Paperwork Reduction Act: New Approaches Can Strengthen Information Collection and Reduce Burden*, [GAO-06-477T](#) (Washington, D.C.: Mar. 8, 2006).

¹¹ DHS officials told us that the document was last revised in June 2007. They said that they continued to coordinate the review of the last version of the report within DHS but no further versions were developed.

¹² DHS's report also contains appendices that cover a variety of topics, including the issue of liability as relates to information sharing, for example, the damages the owner of a CIKR facility may face if it did not address

DHS officials said that they did not perform a cost-benefit analysis consistent with Circular A-4 because at the time they were required to do the report, they did not have quantifiable data to do such an analysis. They further explained that DHS was developing the report while DHS's Information Analysis and Infrastructure Protection group (now IP) was in the process of being established and prior to DHS's development of an accepted framework for compiling security and vulnerability information and assessing risk. In the absence of this framework, the officials said that contractor staff was tasked to compile material from published unclassified sources on the existing regulatory structure in the 17 sectors and draft the report, which was reviewed by DHS staff. They also said that DHS updated the report in 2007 to account for changes that had taken place since 2005, including a statutory requirement that DHS issue regulations requiring vulnerability assessments for certain chemical facilities and the development and implementation of site security plans for those facilities.¹³ DHS officials also noted that the interim NIPP was available while the draft was being prepared and it was used to help guide the development of the final report.

DHS officials told us that they believe the final report was useful because it provided insights on different regulatory approaches across sectors and used appendixes to present more detailed regulatory overviews of three sectors—the chemical sector, the electricity sub sector of the energy sector, and the food and agriculture sector. They added that some sectors used this information to help write sector specific plans (SSPs) that are to augment the NIPP and detail the application of the NIPP framework to each CIKR sector.¹⁴ Nonetheless, DHS officials said that they believe that the report is outdated because DHS's CIKR program has evolved and matured since the report was originally completed, including DHS's efforts to promote and achieve voluntary information sharing between DHS and the private sector. Regarding the latter, DHS officials stated that they believe that the type of report directed by the Conference Report—that DHS analyze whether private sector entities should be required to provide information to the department—conflicts with the partnering/voluntary information-sharing approach DHS was already mandated to pursue under the Homeland Security Act.¹⁵

In February 2009, DHS provided us with a separate document referred to as the *Executive Summary: Update of the Cost Benefit Report*. This document included an elaboration of how DHS's partnering arrangement has evolved since the 2005 report was undertaken. This evolution occurred via the formation and continued maturation of the SSA concept, where the federal departments and agencies identified in HSPD-7 as responsible for CIKR protection activities in specified CIKR sectors lead the coordination effort for CIKR protection in those sectors; the

identified vulnerabilities if an incident occurred; the applicability of different regulatory structures to critical infrastructure protection; and various approaches to the conduct of cost-benefit analysis.

¹³ See Pub. L. No. 109-295, § 550, 121 Stat. 1355, 1388-89 (2006).

¹⁴ Sector Specific Plans are to be developed by the sector specific agencies in collaboration with other sector partners.

¹⁵ See Pub. L. No. 107-296, § 214, 116 Stat. at 2152-55. See also 71 Fed. Reg. 52,262 (Sept. 1, 2006) (establishing uniform procedures for the voluntary sharing of critical infrastructure information with DHS) (codified at 6 C.F.R. pt. 29).

formation of government and sector coordinating councils (GCCs and SCCs);¹⁶ and the issuance of critical infrastructure protection planning documents, including the NIPP and SSPs. Officials identified several other mechanisms that have been developed to share CIKR information and improve critical information protection. These include the CIKR Information Sharing Environment that is designed to address the complex requirements of information sharing among diverse sectors having different characteristics such as ownership patterns, history of collaboration, types and extent of interdependencies, and regulatory requirements. According to DHS, the Infrastructure Analysis and Strategy Division and DHS's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)¹⁷ have undertaken activities to enhance the ability of the private sector to prevent, protect against, and respond to terrorist attacks and all-hazards incidents impacting CIKR. These activities include individual sector threat assessments and the development of a common risk model to be deployed across all sectors to evaluate risks associated with infrastructure security.¹⁸ We did not evaluate whether these actions are adequate to address the CIKR security and vulnerability concerns that led to the conference report language directing DHS to do the cost-benefit report. Such a study on our part would entail, among other things, a closer examination of the sources used by DHS to obtain cost and benefit information, including whether alternative sources or methods would yield more complete data, and discussions with representatives from some or all of the CIKR sectors to assess the completeness and appropriateness of the DHS approach—which is beyond the scope of this review.

As discussed with your staff, because the DHS report is several years old and given DHS's evolving approach to CIKR partnering that it reports has improved CIKR information sharing and security, further analysis of the report would not be beneficial. Therefore, this correspondence represents the fulfillment of our responsibility as directed in Conference Report 108-774.

¹⁶ The GCC comprises representatives across various levels of government (federal, state, local, tribal, and territorial) as appropriate to the security and operational landscape of each individual sector. The SCC is the private sector counterpart to the GCC. These councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. SCCs serve as the government's principal point of entry into each sector for developing and coordinating a wide range of CIKR protection activities and issues.

¹⁷ According to DHS, HITRAC is a joint infrastructure intelligence fusion center that combines the expertise of IP's Infrastructure Analysis and Strategy Division with that of the Office of Intelligence and Analysis in the Critical Infrastructure Threat Analysis Division. DHS officials said that HITRAC is to manage a range of analytic activities of Federal, State, local, and private sector decision-makers by integrating a variety of models, methodologies, and analytic techniques.

¹⁸ GAO has conducted evaluations of risk modeling, for example, see *Highway Infrastructure: Federal Efforts to Strengthen Security Should be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure*, GAO-09-57, (Washington, D.C.: January 2009) and *Emergency Transit Assistance: Federal Funding for Recent Disasters and Options for the Future*, GAO-08-243, (Washington, D.C.: February 2008).

Agency Comments and Our Evaluation

We requested comments on a draft of this report from the Secretary of Homeland Security. DHS provided written comments on June 17, 2009 which are summarized below and reprinted in Enclosure II.

In its comments, DHS did not state whether it concurred with the contents of the draft report but emphasized that the primary basis for the approach taken in 2005 to develop the cost-benefit report was to assure that the Department's mandated public-private partnership building activity be performed without disruption. It said that a data collection effort to identify costs and benefits for a regulatory approach to collecting information from the private sector would have stopped this process with questionable success at acquiring the information. DHS added that the PRA was not the primary factor in the approach chosen as suggested in the draft report. We have revised language in the report to clarify that the PRA was, according to DHS, a contributing factor, not the primary factor, in making the decision about which approach to choose. Finally, DHS reiterated that the cost-benefit report has proved beneficial to DHS because it helped shape the development of the regulatory process put into place for selected chemical facilities and provided the basis for developing the current CIKR information sharing environment. DHS also provided technical comments which we have incorporated where appropriate.

- - - - -

We will send copies of this correspondence to the Secretary of Homeland Security and interested congressional committees and subcommittees. We will also make copies available to others on request. In addition, this report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff has any questions about this report or wish to discuss the matter further, please contact me at (202) 512-8777 or caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. In addition to the contact named above, John Mortin, Assistant Director and Tony DeFrank, Analyst-in-Charge, managed this assignment. Chuck Bausell assisted with design and methodology. Thomas Lombardi provided legal support and Katherine Davis provided assistance in report preparation.

Sincerely,



Stephen L. Caldwell
Director, Homeland Security and Justice Issues

Enclosures

Enclosure I

Sector-Specific Agencies (SSAs), and Critical Infrastructure and Key Resource (CIKR) Sectors

The *National Infrastructure Protection Plan* (NIPP) provides a framework for organizing and managing risk to the U.S.’s CIKR. The NIPP outlines the roles and responsibilities of the Department of Homeland Security (DHS) and other security partners—including other federal agencies, state, territorial, local, and tribal governments, and private companies. Within the NIPP framework, DHS is responsible for leading and coordinating the overall national effort to enhance protection via 18 CIKR sectors. The NIPP assigns responsibility for CIKR sectors to SSAs. As an SSA, DHS has direct responsibility for leading, integrating, and coordinating efforts of security partners to protect 11 CIKR sectors. The remaining sectors are led by eight other federal agencies. The following lists the SSAs and their sectors.

| Sector Specific Agency | Critical Infrastructure and Key Resource Sector |
|---|--|
| Departments of Agriculture ^a and Health and Human Services ^b | Agriculture and Food |
| Department of Defense ^c | Defense Industrial Base |
| Department of Energy | Energy ^d |
| Department of Health and Human Services | Healthcare and Public Health |
| Department of the Interior | National Monuments and Icons |
| Department of the Treasury | Banking and Finance |
| Environmental Protection Agency | Water ^e |
| Department of Homeland Security <ul style="list-style-type: none"> <li data-bbox="321 1081 938 1192">• Office of Infrastructure Protection <li data-bbox="321 1201 938 1257">• Office of Cyber Security and Communications <li data-bbox="321 1266 938 1293">• Transportation Security Administration <li data-bbox="321 1302 938 1358">• Transportation Security Administration and U. S. Coast Guard^f <li data-bbox="321 1367 938 1415">• Immigration and Customs Enforcement, Federal Protective Service | Commercial Facilities; Critical Manufacturing; Emergency Services; Nuclear Reactors, Materials, and Waste; Dams; and Chemical Sectors Information Technology and Communications Sectors Postal and Shipping Transportation Systems ^g Government Facilities ^h |

Source: 2009 National Infrastructure Protection Plan

a The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

b The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.

c Nothing in the NIPP impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DoD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

d The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.

e The Water Sector includes drinking water and wastewater systems.

f The U.S. Coast Guard is the SSA for the maritime transportation mode.

g In accordance with HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

h The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

Enclosure II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

June 17, 2009

Mr. Stephen L. Caldwell
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Caldwell:

RE: Draft Report GAO-09-654R, The Department of Homeland Security's Critical Infrastructure Protection Cost-Benefit Report (GAO Job Code 440794)

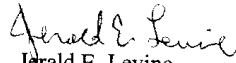
Thank you for the opportunity to review and comment on the draft report referenced above. Department of Homeland Security (DHS) officials recognize the short timeframe your team had to fulfill responsibilities under the Conference Report 108-774 reporting requirement on the costs and benefits of mandating private sector security measure and vulnerability reporting that accompanied the Department of Homeland Security Appropriations Act, 2005. National Protection and Programs Directorate (NPPD) officials appreciated your team's professionalism in conducting this review in an efficient a way as possible to collect the information needed.

The draft report contains no recommendations but summarizes and documents DHS's approach to developing this report. NPPD officials separately provided specific technical comments as suggestions for enhancing the draft report's clarity and accuracy. Officials re-emphasize that the primary basis for the approach taken in 2005 to develop the Cost-Benefit Report was to assure that the Department's mandated public-private partnership building activity be performed without disruption. A data collection effort to identify costs/benefits for a regulatory approach to collecting information from private sector would have stopped the process with questionable success at acquiring the information. The Paperwork Reduction Act was a factor but not the primary factor as the draft suggests.

The draft report describes the information sharing programs that NPPD staff discussed with the U.S. Government Accountability Office (GAO) team that have evolved from a public-private partnership foundation since 2005. Information from the Cost-Benefit Report helped to shape the development of the regulatory process that was put in place for selected chemical facilities and the development and implementation of site security plans for those facilities. In addition, the framework laid out in the Cost-Benefit report provided the basis for the development of the current Critical Infrastructure and Key Resource (CIKR) Information Sharing Environment described in the draft report. This CIKR Environment has since been adopted as the primary private sector component of the National Information Sharing

Environment by the Program Manager of the Information Sharing Environment, the Federal Office established under the 2002 Intelligence Reform and Terrorist Prevention Act to improve information sharing across the Federal government and with its security stakeholders. Consequently, the effort to develop the Cost-Study Report has proved beneficial.

Sincerely,



Gerald E. Levine

Director

Departmental GAO/OIG Audit Liaison Office

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

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

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548