United States Government Accountability Office

Testimony

Before the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee of the Homeland Security Committee, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
October 7, 2015

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

Factors to Consider when Reorganizing

Statement of Chris Currie, Director
Homeland Security and Justice

Accessible Version

October 2015

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

Factors to Consider when Reorganizing

GAO Highlights

Highlights of GAO-16-140T, a testimony before the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee of the Homeland Security Committee, House of Representatives

Why GAO Did This Study

NPPD is the DHS component responsible for addressing physical and cyber infrastructure protection, a mission area of critical importance in today's threat environment. Critical infrastructure owners and operators continue to experience increasingly sophisticated cyber intrusions and a "cyber-physical convergence" has changed the risks to critical infrastructure ranging from energy and transportation to agriculture and health care, according to a DHS strategic review.

NPPD's potential reorganization is the latest in DHS's organizational evolution. In 2003, GAO designated implementing and transforming DHS as high risk because DHS had to transform 22 agencies—several with major management challenges—into one department. The overriding tenet has consistently remained DHS's ability to build a single, cohesive, and effective department that is greater than the sum of its parts—a goal that requires effective collaboration and integration of its various components and management functions. This statement describes key factors for consideration in a NPPD reorganization. It includes observations from GAO's prior work on organizational change, reorganization, and transformation, applicable themes from GAO's high risk list, and NPPD related areas from GAO's work in assessing programmatic duplication, overlap, and fragmentation.

This testimony is based on reports we issued from 2003 through 2015.

View GAO-16-140T. For more information, contact Chris Currie at (404) 679-1875 or curriec@gao.gov.

What GAO Found

GAO's prior work includes four areas for agency officials' consideration when evaluating or implementing a reorganization or transformation.

First, GAO reported in May 2012 on key questions to consider when evaluating an organizational change that involves consolidation, such as what are the goals of the consolidation and how have stakeholders been involved in the decision-making? For reorganization implementation, GAO's prior findings reported in July 2003 include lessons learned from the experiences of large private and public sector organizations. The resulting practices GAO developed include ensuring that top leadership drives the transformation and establishing a communication strategy to create shared expectations and report related progress.

Second, GAO reported in March 2012 that successful government reorganizations balanced executive and legislative roles. Specifically, GAO reported that all key players should be engaged in discussions about reorganizing government: the President, Congress, and other parties with vested interests. It is important that consensus is obtained on identified problems and needs, and that the solutions the U.S. government legislates and implements can effectively remedy the problems the nation faces in a timely manner. Fixing the wrong problems, or even worse, fixing the right problems poorly, could cause more harm than good.

Third, GAO's applicable high-risk work identifies areas that agency officials should consider as part of a reorganization. For example, one high-risk area is securing cyber critical infrastructure and federal information systems and protecting the privacy of personally identifiable information. Specifically, safeguarding the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—is a continuing concern cited in GAO's 2015 High Risk Series Update report. Given the National Protection and Programs Directorate's (NPPD) current cybersecurity activities, addressing these concerns in any reorganization effort would be critical. For example, NPPD conducts analysis of cyber and physical critical infrastructure interdependencies and the impact of a cyber threat or incident to the Nation's critical infrastructure. Sustained attention to this function is vitally important.

Fourth, GAO has identified areas where agencies may be able to achieve greater efficiency or effectiveness by reducing programmatic duplication, overlap, and fragmentation. Since 2011, GAO has reported annually on this topic. Several of its findings in the reports relate to DHS and NPPD activities. For example, in 2015 GAO reiterated a September 2014 recommendation that DHS should mitigate potential duplication or gaps by consistently capturing and maintaining data from overlapping vulnerability assessments of critical infrastructure and improving data sharing and coordination among the offices and components involved with these assessments, of which NPPD is one. DHS agreed with the recommendation. Attention to potential programmatic overlap, duplication, and fragmentation during an NPPD reorganization could improve the agency's overall efficiency.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee:

I am pleased to be here today to discuss our observations on the potential reorganization of the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD). NPPD is the DHS component responsible for addressing physical and cyber infrastructure protection, a mission area of critical importance in today's threat environment. Critical infrastructure owners and operators continue to experience increasingly sophisticated cyber intrusions and a "cyber-physical convergence" has changed the risks to critical infrastructure ranging from energy and transportation to agriculture and health care, according to a DHS strategic review.[1]

NPPD's potential reorganization is the latest in DHS's organizational evolution. In 2003, we designated implementing and transforming DHS as high risk because DHS had to transform 22 agencies—several with major management challenges—into one department.[2] Further, failure to effectively address DHS's management and mission risks could have serious consequences for U.S. national and economic security. Over the past 12 years, the focus of this high-risk area has evolved in tandem with DHS's maturation and evolution. The overriding tenet has consistently remained DHS's ability to build a single, cohesive, and effective department that is greater than the sum of its parts—a goal that requires effective collaboration and integration of its various components and management functions.

You asked us to offer our perspectives on reorganizations, given anticipated but unspecified changes planned at NPPD. This statement describes key factors for consideration in a NPPD reorganization. It includes observations from our prior work on organizational change, reorganization, and transformation, applicable themes from GAO's high risk list, and NPPD related areas from our work in assessing programmatic duplication, overlap, and fragmentation.

[1]DHS, *The 2014 Quadrennial Homeland Security Review* (Washington, D.C.: June 2014).

[2]GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

This testimony is based on reports we issued from 2003 through 2015.[3] For this work, among other things, we convened a forum to identify and discuss useful practices and lessons learned from major private and public sector organizational mergers, acquisitions, and transformations; conducted interviews with knowledgeable officials; reviewed relevant literature and agency documentation; reviewed the status of high risk issues; and identified material in our routine audit work where areas of potential fragmentation, overlap, and duplication were identified. Recurring themes and findings from those data gathering efforts are summarized in the published reports. More detailed information on our scope and methodology appears in the published reports.

We conducted the work upon which this statement is based 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.

Background

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.[4] For example, the Act required DHS to develop a comprehensive national plan for securing the nation's critical infrastructure and key resources, including power production, generation and distribution systems, and information technology and telecommunication systems,

[3]GAO, *Streamlining Government: Questions to Consider When Evaluating Proposals to Consolidate Physical Infrastructure and Management Functions*, GAO-12-542 (Washington, D.C.: May 23, 2012); GAO, *Government Efficiency and Effectiveness: Opportunities for Improvement and Considerations for Restructuring*, GAO-12-454T (Washington, D.C.: March 21, 2012); GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015); GAO, *2015 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, GAO-15-404SP (Washington, D.C.: April 14, 2015); GAO, Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations, GAO-03-669 (Washington, D.C.: July 2, 2003).

[4]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.

among others.[5] Homeland Security Presidential Directive (HSPD) 7 further defined critical infrastructure protection responsibilities for DHS and other departments.[6] For example, HSPD-7 directed DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across critical infrastructure sectors. Various other statutes and directives provide specific legal authorities for infrastructure protection and resiliency programs.[7]

NPPD was established in 2007 as DHS evolved. Specifically, after the Post-Katrina Emergency Management Reform Act of 2006 transferred to the Federal Emergency Management Agency most of what was then termed the Preparedness Directorate, the Secretary of Homeland Security at that time created NPPD. NPPD combined most of the remaining functions of the Preparedness Directorate, such as the Office

[5]See 6 U.S.C. § 121(d)(5). "Critical infrastructure" are 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. 42 U.S.C. § 5195c(e). Key resources are publicly or privately controlled resources essential to minimal operations of the economy or government. 6 U.S.C. § 101(10).

[6]Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection* (Dec. 17, 2003).

[7]For example, the Cyber Security Research and Development Act, enacted in January 2002, authorized funding through fiscal year 2007 for the National Institute of Standards and Technology and the National Science Foundation to facilitate increased research and development for computer and network security and to support related research fellowships and training. See generally Pub. L. No. 107-305, 116 Stat. 2367 (2002). Other critical infrastructure-related presidential directives include HSPD-3, which addresses implementation of the Homeland Security Advisory System; HSPD-9, which establishes a national policy to defend the nation's agriculture and food system; HSPD-10, which addresses U.S. efforts to prevent, protect against, and mitigate biological weapons attacks perpetrated against the United States and its global interests; HSPD-19, which addresses the prevention and detection of, protection against, and response to terrorist use of explosives in the United States; HSPD-20, which addresses the establishment of a comprehensive and effective national continuity policy; and HSPD-22, which, as described in the NIPP, addresses the ability of the United States to prevent, protect, respond to, and recover from terrorist attacks employing toxic chemicals. Presidential Policy Directive/PPD-21—*Critical Infrastructure Security and Resilience*—issued February 12, 2013, revoked HSPD-7 but provided that plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded.

of Infrastructure Protection, with other functions.[8] For example, the Office of Cyber Security and Telecommunications combined with the National Communications System and the new Office of Emergency Communications and was renamed the Office of Cyber Security and Communications. As reported in DHS's fiscal year 2016 budget request, NPPD employs approximately 3,500 staff. NPPD's current organizational structure includes five divisions.

- The Federal Protective Service is the agency charged with protecting and delivering law enforcement to and protection services for federal facilities.
- The Office of Biometric Identity Management, formerly US-VISIT, provides biometric identity services to DHS and its mission partners.
- The Office of Cybersecurity and Communications has the mission of assuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure.
- The Office of Cyber and Infrastructure Analysis provides consolidated all-hazards consequence analysis focusing on cyber and physical critical infrastructure interdependencies and the impact of a cyber threat or incident to the Nation's critical infrastructure.
- The Office of Infrastructure Protection leads the coordinated national effort to reduce risk to critical infrastructure posed by acts of terrorism.

Many of NPPD's activities are guided by the 2013 National Infrastructure Protection Plan (NIPP). NPPD issues the NIPP in accordance with requirements set forth in the Homeland Security Act, as amended, HSPD-7, and more recently Presidential Policy Directive-21—*Critical Infrastructure Security and Resilience*. The NIPP was developed through a collaborative process involving critical infrastructure stakeholders. Central to the NIPP is managing the risks from significant threat and hazards to physical and cyber critical infrastructure, requiring an integrated approach to:

- Identify, deter, detect, disrupt, and prepare for threats and hazards to the Nation's critical infrastructure;

[8] See 6 U.S.C. § 315. See also 6 U.S.C. § 452 (authorizing the Secretary to allocate or reallocate functions among the officers of the Department, and to establish, consolidate, alter, or discontinue organizational units within the Department).

- Reduce vulnerabilities of critical assets, systems, and networks; and
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

Key Factors for Consideration in a NPPD Reorganization

Our prior work includes four areas that offer valuable insights for agency officials to consider when evaluating or implementing a reorganization or transformation. These areas include (1) considering key questions for consolidation decision-making and factors for success when implementing an organizational change; (2) balancing executive and congressional roles in the decision-making process; (3) considering themes and findings in our DHS high risk work; and (4) addressing any related duplication, overlap, or fragmentation of existing programs.

Key Questions to Consider During Organizational Consolidation and Practices for Transformation Implementation

Two sets of considerations for organizational transformations provide insights for NPPD's organizational change decision-making and implementation. First, in May 2012, we reported on key questions for agency officials to consider when evaluating an organizational change that involves consolidation.[9] Table 1 provides a summary of these key questions from our previous work on organizational transformations, which we developed through a review of selected consolidation initiatives at the federal agency level, among other things. Attention to these factors would provide NPPD with assurance that important aspects of effective organizational change are addressed.

[9]GAO-12-542.

Table 1: Key questions from prior work on evaluating and implementing organizational change that involves consolidation

Key Questions
What are the goals of the consolidation? What opportunities will be addressed through the consolidation and what problems will be solved? What problems, if any, will be created?
What will be the likely costs and benefits of the consolidation? Are sufficiently reliable data available to support a business-case analysis or cost-benefit analysis?
How can the up-front costs associated with the consolidation be funded?
Who are the consolidation stakeholders, and how will they be affected? How have the stakeholders been involved in the decision, and how have their views been considered? On balance, do stakeholders understand the rationale for consolidation?
To what extent do plans show that change management practices will be used to implement the consolidation?

Source: GAO-12-542.

Second, as DHS was formed, we reported in July 2003 on key practices and implementation steps for mergers and organizational transformations. The factors listed in table 2 were built on the lessons learned from the experiences of large private and public sector organizations. The resulting practices we developed are intended to help agencies transform their cultures so that they can be more results oriented, customer focused, and collaborative in nature. As NPPD reorganizes, consulting each of these practices would ensure that lessons learned from other organizations are considered.

Table 2. Key Practices and Implementation Steps for Mergers and Organizational Transformations

Key Factors When Implementing Organizational Change	Implementation Step
Ensure top leadership drives the transformation.	• Define and articulate a succinct and compelling reason for change. • Balance continued delivery of services with merger and transformation activities.
Establish a coherent mission and integrated strategic goals to guide the transformation	Adopt leading practices for results-oriented strategic planning and reporting.
Focus on a key set of principles and priorities at the outset of the transformation.	Embed core values in every aspect of the organization to reinforce the new culture.
Set implementation goals and a timeline to build momentum and show progress from day one.	• Make public implementation goals and timeline. • Seek and monitor employee attitudes and take appropriate follow-up actions. • Identify cultural features of merging organizations to increase understanding of former work environments. • Attract and retain key talent. • Establish an organization-wide knowledge and skills inventory to exchange knowledge among merging organizations.
Dedicate an implementation team to manage the transformation process.	• Establish networks to support implementation team. • Select high-performing team members.

Key Factors When Implementing Organizational Change	Implementation Step
Use the performance management system to define responsibility and assure accountability for change.	Adopt leading practices to implement effective performance management systems with adequate safeguards.
Establish a communication strategy to create shared expectations and report related progress.	• Communicate early and often to build trust. • Ensure consistency of message. • Encourage two-way communication. • Provide information to meet specific needs of employees.
Involve employees to obtain their ideas and gain their ownership for the transformation.	• Use employee teams. • Involve employees in planning and sharing performance information. • Incorporate employee feedback into new policies and procedures. • Delegate authority to appropriate organizational levels.
Build a world-class organization.	Adopt leading practices to build a world-class organization.

Source: GAO-03-669.

Balancing Executive and Congressional Roles in Reorganization Decision-making

In March 2012, we found that successful government reorganizations balanced executive and legislative roles and that all key players engaged in discussions about reorganizing government: the President, Congress, and other parties with vested interests, including state and local governments, the private sector, and citizens.[10] It is important that consensus is obtained on identified problems and needs, and that the solutions our government legislates and implements can effectively remedy the problems we face in a timely manner. Fixing the wrong problems, or even worse, fixing the right problems poorly, could cause more harm than good.

We found that it is imperative that Congress and the administration form an effective working relationship on restructuring initiatives. Any systemic changes to federal structures and functions should be approved by Congress and implemented by the executive branch, so each has a stake in the outcome. In addition, Congressional deliberative processes serve the vital function of both gaining input from a variety of clientele and stakeholders affected by any changes and providing an important constitutional check and counterbalance to the executive branch.

[10]GAO-12-454T.

Applicable GAO High Risk Work

Securing Cyber Critical Infrastructure and Federal Information Systems and Protecting the Privacy of Personally Identifiable Information

Safeguarding the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—is a continuing concern cited in our 2015 High Risk Series Update.[11] Given NPPD's current cybersecurity activities, addressing these concerns in any reorganization effort would be critical. For example, NPPD conducts analysis of cyber and physical critical infrastructure interdependencies and the impact of a cyber threat or incident to the Nation's critical infrastructure. Sustained attention to this function is vitally important. In our 2015 High-Risk Series Update report, we note that to address the substantial cyber critical infrastructure risks facing the nation, executive branch agencies, in particular DHS, need to continue to enhance their cyber analytical and technical capabilities (including capabilities to address federal cross-agency priorities), expand oversight of federal agencies' implementation of information security, and demonstrate progress in strengthening the effectiveness of public-private sector partnerships in securing cyber critical infrastructures.

In our 2015 High Risk Series Update report, we highlight two additional high risk areas related to securing cyber critical infrastructure. The security of our federal cyber assets has been on our list of high-risk areas since 1997. In 2003, we expanded this high-risk area to include the protection of critical cyber infrastructure. This year, we added protecting the privacy of personally identifiable information (PII)—information that is collected, maintained, and shared by both federal and nonfederal entities.

Strengthening DHS Management Functions

Our 2015 High-Risk Series Update found that DHS made significant progress in addressing our concerns, but that considerable work remains in several areas. To the extent that these issues are relevant to a reorganized NPPD, consideration of each area would be important so as not to jeopardize DHS's progress in taking steps toward addressing its implementation and transformation as a high-risk area. These areas of concern include:

- *Acquisition management*. DHS has taken a number of actions to establish effective component-level acquisition capability, such as initiating assessments of component policies and processes for managing acquisitions. In addition, DHS is working to assess and

[11] GAO-15-290.

address whether appropriate numbers of trained acquisition personnel are in place at the department and component levels, an outcome it has partially addressed. Further, while DHS has initiated efforts to demonstrate that major acquisition programs are on track to achieve their cost, schedule, and capability goals, DHS officials have acknowledged it will be years before this outcome has been fully addressed. Much of the necessary program information is not yet consistently available or up to date. Attention to effective acquisition management is particularly important in a NPPD reorganization, given the substantial costs for cybersecurity programmatic efforts. For example, NPPD's National Cybersecurity Protection System, intended to defend the federal civilian government's information technology infrastructure from cyber threats, had a lifecycle cost of $5.7 billion as of January 2015.

- *IT management.* While the Department obtained a clean opinion on its financial statements, in November 2014, the department's financial statement auditor reported that continued flaws in security controls such as those for access controls, configuration management, and segregation of duties were a material weakness for fiscal year 2014 financial reporting. Thus, the department needs to remediate the material weakness in information security controls reported by its financial statement auditor.
- *Financial management.* We reported in September 2013 that DHS needs to modernize key components' financial management systems and comply with financial management system requirements. The components' financial management system modernization efforts are at various stages due, in part, to a bid protest and the need to resolve critical stability issues with a legacy financial system before moving forward with system modernization efforts. Without sound controls and systems, DHS faces long-term challenges in ensuring its financial management systems generate reliable, useful, and timely information for day-to-day decision making.
- *Human capital management.* The Office of Personnel Management's 2014 Federal Employee Viewpoint Survey data showed that DHS's scores continued to decrease in all four dimensions of the survey's index for human capital accountability and assessment—job satisfaction, talent management, leadership and knowledge management, and results-oriented performance culture. Morale problems are particularly an issue among NPPD employees, who report some of the lowest morale scores among federal agency subcomponents. DHS has taken steps to identify where it has the most significant employee satisfaction problems and developed plans

to address those problems. In September 2012, we recommended, among other things, that DHS improve its root-cause analysis efforts related to these plans. As of February 2015, DHS reported actions underway to address our recommendations but had not fully implemented them. Given the sustained decrease in DHS employee morale indicated by Federal Employee Viewpoint Survey data, it is particularly important that DHS fully implement these recommendations and thereby help identify appropriate actions to take to improve morale within its components and department wide. In addition, given NPPD's low morale scores, attention to employee concerns during reorganization is crucial to engaging employees in accomplishing NPPD's missions.

- *Management integration.* The Secretary's April 2014 Strengthening Departmental Unity of Effort memorandum highlighted a number of initiatives designed to allow the department to operate in a more integrated fashion, such as the Integrated Investment Life Cycle Management initiative, to manage investments across the department's components and management functions. DHS completed its pilot for a portion of this initiative in March 2014 and, according to DHS's Executive Director for Management Integration, has begun expanding its application to new portfolios, such as border security and information sharing, among others. However, given that these main management integration initiatives are in the early stages of implementation and contingent upon DHS following through with its plans, it is too early to assess their impact. To achieve this outcome, DHS needs to continue to demonstrate sustainable progress integrating its management functions within and across the department and its components.

Related GAO Work on Duplication, Overlap, or Fragmentation

Our prior work identified areas where agencies may be able to achieve greater efficiency or effectiveness by reducing programmatic duplication, overlap, and fragmentation.[12] Since 2011, we have reported annually on this topic, presenting nearly 200 areas wherein opportunities existed for

[12]Fragmentation refers to those circumstances in which more than one federal agency (or more than one organization within an agency) is involved in the same broad area of national need and opportunities exist to improve service delivery. Overlap occurs when multiple agencies or programs have similar goals, engage in similar activities or strategies to achieve them, or target similar beneficiaries. Duplication occurs when two or more agencies or programs are engaged in the same activities or provide the same services to the same beneficiaries.

executive branch agencies or Congress to reduce, eliminate, or better manage fragmentation, overlap, or duplication; achieve costs savings; or enhance revenue. Several of our findings in the reports relate to DHS and NPPD activities. For example, consistent with a previous recommendation with which DHS agreed, in 2015 we reported that DHS could mitigate potential duplication or gaps by consistently capturing and maintaining data from overlapping vulnerability assessments of critical infrastructure and improving data sharing and coordination among the offices and components involved with these assessments, of which NPPD is one.[13] Also, in 2012, we found that federal facility risk assessments were duplicative, as they were conducted by multiple federal agencies, including NPPD's Federal Protective Service (FPS). We recommended that DHS should work with federal agencies to determine their reasons for duplicating the activities included in FPS's risk assessments and identify measures to reduce this duplication.[14] DHS did not comment on whether it agreed with this recommendation at the time it was made and the recommendation was not fully addressed as of March 2015. Addressing these duplication concerns and any other fragmentation, overlap, or unnecessary duplication that agency officials may identify as part of its reorganization will improve the agencies' overall efficiency and effectiveness.

Given the critical nature of NPPD's mission, considering key factors from our previous work would help inform a reorganization effort. For example, the lessons learned by other organizations involved in substantial transformations could provide key insights for agency officials as they consider and implement reorganization. Attention to these and the other factors we identified would improve the chances of a successful NPPD reorganization.

Chairman Ratcliffe, Ranking Member Richmond, and members of the subcommittee, this concludes my prepared statement. I would be happy to respond to any questions you may have.

[13]GAO-15-404SP and GAO, *Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts*, GAO-14-507 (Washington, D.C.: Sept. 15 2014).

[14]GAO-12-342SP.

GAO Contacts and Staff Acknowledgements

If you or your staff members have any questions about this testimony, please contact me at (404) 679-1875 or curriec@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Other contributors include: Ben Atwater and Adam Gomez.

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 website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://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 website, 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.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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