United States Government Accountability Office

GAO

Report to Congressional Requesters

June 2010

CYBERSECURITY

Key Challenges Need to Be Addressed to Improve Research and Development

GAO
Accountability ★ Integrity ★ Reliability

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-10-466, a report to congressional requesters

June 2010

CYBERSECURITY

Key Challenges Need to Be Addressed to Improve Research and Development

Why GAO Did This Study

Computer networks and infrastructures, on which the United States and much of the world rely to communicate and conduct business, contain vulnerabilities that can leave them susceptible to unauthorized access, disruption, or attack. Investing in research and development (R&D) is essential to protect critical systems and to enhance the cybersecurity of both the government and the private sector. Federal law has called for improvements in cybersecurity R&D, and, recently, President Obama has stated that advancing R&D is one of his administration's top priorities for improving cybersecurity.

GAO was asked to determine the key challenges in enhancing national-level cybersecurity R&D efforts among the federal government and private companies. To do this, GAO consulted with officials from relevant federal agencies and experts from private sector companies and academic institutions as well as analyzed key documents, such as agencies' research plans.

What GAO Recommends

GAO is recommending that the Director of OSTP direct NITRD to exercise its leadership responsibilities by taking several actions, including developing a national agenda, and establishing and utilizing a mechanism to keep track of federal cybersecurity R&D funding. OSTP agreed with GAO's recommendation and provided details on planned actions.

View GAO-10-466 or key components.
For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov, or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Several major challenges impede efforts to improve cybersecurity R&D. Among the most critical challenges are the following:

Establishing a prioritized national R&D agenda. While R&D that is in support of specific agencies' missions is important, it is also essential that national research efforts be strategically guided by an ordered set of national-level R&D goals. Additionally, it is critical that cyberspace security research efforts are prioritized across all sectors to ensure that national goals are addressed. Accordingly, the National Strategy to Secure Cyberspace recommended that the Office of Science and Technology Policy (OSTP) coordinate the development of an annual cybersecurity research agenda that includes near-term (1-3 years), mid-term (3-5 years), and long-term (5 years or longer) goals. Although OSTP has taken initial steps toward developing such an agenda, one does not currently exist. OSTP and Office of Management and Budget officials stated that they believe an agenda is contained in existing documents; however, these documents are either outdated or lack appropriate detail. Without a current national cybersecurity R&D agenda, the nation is at risk that agencies and private sector companies may focus on their individual priorities, which may not be the most important national research priorities.

Strengthening leadership. While officials within OSTP's Subcommittee on Networking and Information Technology Research and Development (NITRD)—a multiagency coordination body that is primarily responsible for providing leadership in coordinating cybersecurity R&D—have played a facilitator role in coordinating cybersecurity R&D efforts within the federal government, they have not led agencies in a strategic direction. NITRD's lack of leadership has been noted by many experts as well as by a presidential advisory committee that reported that federal cybersecurity R&D efforts should be focused, coordinated, and overseen by a central body. Until NITRD exercises its leadership responsibilities, federal agencies will lack overall direction for cybersecurity R&D.

Tracking R&D funding and establishing processes for the public and private sectors to share key R&D information. Despite a congressional mandate to develop a governmentwide repository that tracks federally funded R&D, including R&D related to cybersecurity, such a repository is not currently in place. Additionally, the government does not have a process to foster the kinds of relationships necessary for coordination between the public and private sectors. While NITRD hosted a major conference last year that brought together public, private, and academic experts, this was a one-time event, and, according to experts, next steps remain unclear. Without a mechanism to track all active and completed cybersecurity R&D initiatives, federal researchers and developers as well as private companies lack essential information about ongoing and completed R&D. Moreover, without a process for industry and government to share cybersecurity R&D information, the nation is at risk of having unforeseen gaps.

Contents

Table

Abbreviations

CNCI	Comprehensive National Cybersecurity Initiative
CSIA IWG	Cyber Security and Information Assurance Interagency Working Group
CSIS	Center for Strategic and International Studies
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
IT	information technology
IT-SCC	Information Technology Sector Coordinating Council
NIST	National Institute of Standards and Technology
NITRD	Subcommittee on Networking and Information Technology Research and Development
NSA	National Security Agency
NSF	National Science Foundation
NSTC	National Science and Technology Council
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PCAST	President's Council of Advisors on Science and Technology
PITAC	President's Information Technology Advisory Committee
R&D	research and development
RaDiUS	Research and Development in the U.S. (database)
SCORE	Special Cyber Operations Research and Engineering

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 3, 2010

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Yvette D. Clarke
Chairwoman
Subcommittee on Emerging Threats,
Cybersecurity, and Science and Technology
Committee on Homeland Security
House of Representatives

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way that our government, our nation, and much of the world communicate and conduct business. However, computers, networks, and their infrastructures are not always designed with security in mind. As a result, public and private systems that support critical operations and infrastructures of the federal government can have significant vulnerabilities[1] that can be exploited by malicious users to gain unauthorized access to systems and obtain sensitive information, commit fraud, disrupt operations, or launch attacks against Web sites.

Because of concerns about these malicious attacks from individuals and groups, it is essential that the United States protect its existing critical systems and at the same time work to get ahead of its adversaries by ensuring that future generations of technology will position the United States to better protect its critical systems from attack. As such, we have designated protecting the federal government's information systems as a

[1] A vulnerability is a flaw or weakness in hardware or software that can be exploited, resulting in a violation of an implicit or explicit security policy.

high-risk area.[2] Research in cybersecurity[3] technology is essential to creating a broader range of choices and more robust tools for building secure, networked computer systems in the federal government and in the private sector. Furthermore, over the past two decades, federal law and policy have called for improvements in the research and development (R&D) of cybersecurity tools and techniques. In May 2009, President Obama announced that advancing R&D is one of his administration's top five priorities for improving cybersecurity.

This report responds to your request that we conduct a review of the nation's current cybersecurity-related R&D efforts. Specifically, our objective was to determine the key challenges to enhancing national-level cybersecurity R&D efforts among the federal government and private companies.

To address this objective, we identified experts from the public and private sectors that conduct or coordinate cybersecurity R&D, including 7 government agencies/entities—the Departments of Defense (DOD), Homeland Security (DHS), and Energy (DOE) and the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Office of Science and Technology Policy (OSTP); 24 private sector entities; and 3 academic institutions (see app. I for the complete list). To obtain information on the key R&D challenges that these entities face, we analyzed documentation, such as agencies' research plans and cybersecurity reports, and interviewed federal and industry experts. We then aggregated the identified challenges and validated the top challenges by asking the experts to rank the challenges in order of importance. Appendix I contains further details of our objective, scope, and methodology.

[2] GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

[3] Cybersecurity refers to the defense against attacks on the information technology infrastructure of an organization or, in this case, of the federal government and agencies. Cybersecurity is intertwined with the physical security of assets—from computers, networks, and their infrastructure to the environment surrounding these systems. While both parts of security are necessary to achieve overall security, this report focuses on protecting software and data from attacks that are electronic in nature and that typically arrive over a data communication link. Cybersecurity is a major concern of both the federal government and the private sector.

We conducted this performance audit from June 2009 to June 2010, 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

The speed, functionality, and accessibility that create the enormous benefits of the computer age can, if not properly controlled, allow individuals and organizations to easily eavesdrop on or interfere with computer operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. As public and private organizations use computer systems to transfer more and greater amounts of money, sensitive economic and commercial information, and critical defense and intelligence information, the likelihood increases that malicious individuals will attempt to penetrate current security technologies, disrupt or disable our nation's critical infrastructures, and use sensitive and critical information for malicious purposes.

Because the threats have persisted and grown, in January 2008, the President began implementing a series of initiatives—commonly referred to as the Comprehensive National Cybersecurity Initiative (CNCI)—aimed primarily at improving DHS and other federal agencies' efforts to protect against intrusion attempts and anticipate future threats.[4] Two of these initiatives are related to improving cybersecurity R&D—one is aimed at improving the coordination of federal cybersecurity R&D, and the other is aimed at developing a plan for advancing the United States' R&D in high-risk, high-return areas. We recently reported that CNCI faces significant challenges, including defining roles and responsibilities and coordinating efforts.[5]

[4] The White House, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

[5] GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338 (Washington, D.C.: Mar. 5, 2010).

Numerous Entities Are Involved in the Cybersecurity Research and Development Arena

Several federal entities oversee and aim to coordinate federal cybersecurity research; private entities have structures in place aimed at coordinating research; and numerous federal agencies and private companies fund or conduct this research.

Federal Oversight and Coordination of Cybersecurity R&D

OSTP and OMB, both in the Executive Office of the President, are responsible for providing high-level oversight of federal R&D, including cybersecurity. OSTP promotes the work of the National Science and Technology Council, which prepares R&D strategies that are intended to be coordinated across federal agencies. The council operates through its committees, subcommittees, and interagency working groups, which coordinate activities related to specific science and technology disciplines.

Table 1 contains a brief description of the roles and responsibilities of the federal organizations and groups involved in the oversight and coordination of cybersecurity research.

Table 1: Federal Organizations Involved in the Oversight and Coordination of Cybersecurity Research

Organization	Description
President's Council of Advisors on Science and Technology (PCAST)	Executive Order 13226 established PCAST in September 2001. Under this order, PCAST was established to advise the President on matters involving science and technology policy and assist the National Science and Technology Council in securing private sector involvement in its activities. The council's members are appointed by the President and originate from industry, education, and research institutions and other nongovernmental organizations. The Director of OSTP serves as a co-chair for the council.
President's Information Technology Advisory Committee (PITAC)	PITAC is made up of industry and academic experts appointed by the President to provide independent expert advice to the President, Congress, and federal agencies on networking and information technology R&D. In September 2005, Executive Order 13385 reassigned the roles and responsibilities of PITAC to PCAST.
National Security Council	The council is the President's principal forum for considering national security and foreign policy matters with his senior national security advisors and cabinet officials. The council is chaired by the President. The Cybersecurity Coordinator and Director of National Intelligence both work with the council.
Cybersecurity Office/U.S. Cybersecurity Coordinator	In December 2009, the President created the Cybersecurity Office within the National Security Council and appointed a U.S. Cybersecurity Coordinator. The coordinator is intended to work closely with the federal Chief Information Officer, the federal Chief Technology Officer, and the National Economic Council.
Office of the Director of National Intelligence	The Office of the Director of National Intelligence was established in April 2005. The head of this office serves as the President's principal intelligence advisor and is intended to establish the intelligence community's priorities with clear and measurable goals and objectives as well as provide leadership on cross-cutting intelligence community issues. According to OSTP officials, this office provides technical and administrative support to the Special Cyber Operations Research and Engineering Interagency Working Group.

Organization	Description
Office of Management and Budget (OMB)	The E-Government Act of 2002 mandated that OMB ensure the development and maintenance of a governmentwide repository and Web site that integrates information about federally funded R&D, including R&D related to cybersecurity. Furthermore, the Director of OMB and the Director of OSTP jointly release an annual memorandum to the heads of executive departments and agencies that specifies high-level R&D budget priorities, one of which is to protect the nation's information infrastructure.
Office of Science and Technology Policy (OSTP)	OSTP serves as a primary advisor to the President for policy formation and budget development on all questions in which science and technology are important elements. The office also leads an interagency effort to develop and implement science and technology policies and budgets that are coordinated across federal agencies.
OSTP's National Science and Technology Council (NSTC)	NSTC, established in 1993, is the principal means for the administration to coordinate science and technology policy among the diverse entities that make up the federal R&D enterprise. OSTP works through NSTC to develop strategies that are coordinated across federal agencies. The council operates through its committees, which include the Committee on Homeland and National Security and the Committee on Technology, among others. Each committee oversees a number of subcommittees and interagency working groups focused on science and technology.
NSTC's Committee on Technology	The Committee on Technology addresses policy matters that cut across agency boundaries and provides a formal mechanism for interagency policy coordination and balanced and comprehensive technology R&D programs. Senior-level representatives from federal departments and agencies comprise the committee. The committee is currently co-chaired by the U.S. Chief Information Officer in OMB and the Chief Technology Officer in OSTP. Several other agencies or components are members of the committee, including the Departments of Homeland Security (DHS), Defense (DOD), Justice, Transportation, and the Treasury; the Central Intelligence Agency; the National Security Agency (NSA); and the Office of the Cyber Security Officer from the National Security Council.
The Committee on Technology's Subcommittee on Networking and Information Technology Research and Development (NITRD)	NITRD is a multiagency coordination program that seeks to ensure continued U.S. technological leadership and accelerate deployment of advanced and experimental information technologies. Subcommittee members include representatives from 15 federal agencies or components, including the National Science Foundation (NSF), DOD, NSA, and National Institute of Standards and Technology (NIST). NITRD is responsible for coordinating the planning, budgeting, and assessment of activities of a multiagency federal NITRD program. This program was chartered under the High-Performance Computing Act of 1991, as amended by the Next Generation Internet Research Act of 1998 and the America COMPETES Act of 2007, to help sustain U.S. leadership in cutting-edge science, engineering, and technology through investments from federal agencies involved in information technology R&D.[a]
National Coordination Office (NCO) for NITRD	NCO is responsible for providing technical and administrative support for the Subcommittee on Networking and Information Technology Research and Development and interagency activities of the NITRD program. This includes helping identify research needs by coordinating interagency meetings as well as conferences and workshops with academia and industry. This office is to aid information dissemination by publishing reports, including reports produced by the PITAC, and the annual supplements to the President's budget.

Organization	Description
Senior Steering Group for Cyber Security	In Spring 2008, a senior steering group was created and added to NITRD, which is intended to provide overall leadership and cybersecurity R&D coordination(CNCI Coordination Plan. The steering group's membership includes the co-chair for NITRD; the director of NCO; and senior representatives of agencies, such as DOD, DHS, National Security Agency, NIST, OSTP, and OMB. Additionally, the group is intended to facilitate closer interaction between classified and unclassified R&D. Accordingly, this group's membership also overlaps with the Special Cyber Operations Research and Engineering Interagency Working Group.
Cyber Security and Information Assurance Interagency Working Group (CSIA IWG)	CSIA IWG was chartered in August 2005 to facilitate greater coordination of federal cybersecurity R&D. The working group reports to NITRD and is responsible for facilitating interagency program planning, developing and periodically updating an interagency roadmap, developing recommendations for establishing federal policies and priorities, summarizing annual activities for the NITRD program's supplement to the President's budget, and identifying potential opportunities for collaboration and coordination. Members include NSF, DOD's research organizations, NSA, the Defense Advanced Research Projects Agency, and NIST. Other participants include the Central Intelligence Agency; the Environmental Protection Agency; the National Aeronautics and Space Administration; the National Institutes of Health; and the Departments of Homeland Security, Energy, Justice, State, Transportation, and the Treasury.
Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group	SCORE was created in Spring 2008 and is intended to work in parallel to the CSIA IWG to coordinate classified cybersecurity R&D. It is operated under OSTP and the Director for National Intelligence. Representatives from the SCORE and CSIA IWG participate together in the Senior Steering Group for Cyber Security.

Source: GAO analysis of Executive Office of the President information.

[a] The High-Performance Computing Act of 1991, Pub. L. No. 102-194, 105 Stat. 1595 (Dec. 9, 1991), was amended by the Next Generation Internet Research Act of 1998, Pub. L. No. 105-305, 112 Stat. 2919 (Oct. 28, 1998), and the America COMPETES Act, Pub. L. No. 110-69, 121 Stat. 572 (Aug. 9, 2007).

Private Sector Cybersecurity R&D Coordination

The private sector also has cybersecurity R&D working groups aimed at better coordinating R&D. Under an existing information-sharing framework within a plan referred to as the *National Infrastructure Protection Plan*,[6] two Sector Coordinating Councils—Financial Services and Information Technology—have R&D working groups. These groups are composed of representatives from companies, associations, and other key sector participants to coordinate strategic activities and communicate broad sector member views associated with cybersecurity R&D throughout their sectors. Specifically, these working groups are charged with conducting annual reviews of R&D initiatives in their sectors and

[6] The *National Infrastructure Protection Plan*, which was published in 2006 and revised in 2009, defines the organizational structures that provide the framework for coordination of critical infrastructure protection efforts at all levels of government as well as within and across private-sector-specific councils. These coordinating councils are composed of the representatives of owners and operators, generally from the private sector.

recommending updates to those priorities based on changes in technology, threats, vulnerabilities, and risk.

Federal Agencies and Private Companies Fund or Conduct Cybersecurity R&D

Five agencies—NSF, DHS, DOD, DOE, and NIST—fund and conduct much of the government's cybersecurity R&D.

According to agency officials, NSF's main cybersecurity R&D program is the Trustworthy Computing Program. This program is to support research and education activities that explore novel frameworks, theories, and approaches toward secure and privacy-preserving systems. According to the Subcommittee on Networking and Information Technology Research and Development's (NITRD) supplement to the 2011 budget, NSF's budget was approximately $71.4 million for cybersecurity R&D.

DHS's R&D efforts are aimed at countering threats to the homeland by making evolutionary improvements to current capabilities and developing revolutionary new capabilities. DHS's cybersecurity R&D program resides in the agency's Science and Technology Directorate. DHS has created R&D tools and made them accessible to the broader research community, such as an experimental research testing environment and a research data repository. In November 2009, DHS issued *A Roadmap for Cybersecurity Research*, which was an attempt to establish a foundation on which a national R&D agenda could be built. Furthermore, it was intended to provide detailed R&D agendas related to specific cybersecurity problems.[7]

Several agencies within DOD have cybersecurity R&D programs. The department's Defense Research and Engineering organization within the Office of the Director provides coordination and oversight and supports certain cybersecurity research activities directly. The office is responsible for DOD's science and technology activities as well as for oversight of research and engineering. Although the department's research organizations (e.g., the Office of Naval Research, the Army Research Laboratory, and the Air Force Research Laboratory) have cybersecurity programs, the largest investments within its cybersecurity R&D are with the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA). DARPA is the central R&D organization for the department, and its cybersecurity R&D budget for fiscal year 2010

[7] Examples of the problems identified by DHS include the following: scalable trustworthy systems, enterprise-level metrics, combating insider threats, global-scale identity management, situational understanding and attack attribution, privacy-aware security, and usable security.

is approximately $144 million.[8] Its mission is to identify revolutionary, high-risk, high-payoff technologies of interest to the military, then to support the development of these technologies through transition. NSA also performs extensive cybersecurity research. Its research programs focus on high-speed encryption and certain defense capabilities, among other things. For fiscal year 2010, the agency's budget was approximately $29 million for cybersecurity R&D. The research is conducted and supported by its National Information Assurance Research Group. In addition to DARPA and NSA, approximately $70 million was budgeted for fiscal year 2010 to the Office of the Secretary of Defense and other research organizations within DOD for additional cybersecurity R&D.

DOE also conducts and funds cybersecurity R&D. Nearly all of DOE's cybersecurity R&D investments are directed toward short-term applications. This work is conducted principally at the national laboratories. DOE reported to NITRD that it had spent $3.5 million on cybersecurity R&D for fiscal year 2010, and requested the same amount for fiscal year 2011. Additionally, DOE conducts cybersecurity R&D for other departments, such as DOD.

NIST's cybersecurity research program is multidisciplinary and focuses on a range of long-term and applied R&D. NIST also conducts security research in support of future standards and guidelines. NIST's fiscal year 2010 budget for cybersecurity was about $29 million. The agency also receives funding from other agencies—such as DHS, the Department of Transportation and the General Services Administration—to work on projects that are consistent with its cybersecurity mission.

In addition, many private sector companies pursue government grants or contracts to conduct cybersecurity R&D on behalf of the government, or they independently self-fund cybersecurity research. The private sector generally conducts cybersecurity R&D in areas with commercial viability, which are focused on developing products to help their customers better secure their systems and networks. For example, representatives from one private sector company stated that they have set up unused computers that attempt to attract hackers for the purpose of analyzing the attacker. Another company is conducting R&D related to the Internet's architecture. According to private sector officials, cybersecurity R&D does not

[8] Budget figures provided to NITRD by agencies to include in its annual supplement to the President's budget do not include funding for classified R&D projects.

necessarily have to be conducted by large companies; some small companies have made large contributions.

Various Entities Have Issued Guidance on Federal Cybersecurity R&D

Various public and private sector entities have issued reports that provide guidance and make recommendations for improvements in the nation's activities related to specific aspects of cybersecurity, including R&D. The following key reports offer guidance and direction related to cybersecurity R&D:

- In February 2003, the White House's *The National Strategy to Secure Cyberspace* identified five national priorities, one of which includes reducing cyberspace threats and vulnerabilities.[9] As part of this priority, the strategy tasked the Director of OSTP with coordinating the development of a federal government R&D agenda for cybersecurity and updating it on an annual basis.

- In February 2005, the President's Information Technology Advisory Committee (PITAC) recommended several changes in the federal government's cybersecurity R&D portfolio.[10] One of the report's recommendations was to strengthen coordination and oversight of federal cybersecurity efforts.

- The President's Council of Advisors on Science and Technology (PCAST) found in its 2007 report, entitled *Leadership Under Challenge: Information Technology R&D in a Competitive World*, that the existing federal networking and information technology R&D portfolio was unbalanced in favor of low-risk, small-scale, and short-term efforts.[11] The council recommended that federal agencies increase support for larger-scale, longer-term R&D.

- In December 2008, the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency issued a series of recommendations for a comprehensive national approach to

[9] The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

[10] President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization* (Arlington, Va.: Feb. 28, 2005).

[11] President's Council of Advisors on Science and Technology, *Leadership Under Challenge: Information Technology R&D in a Competitive World* (Washington, D.C.: Aug. 10, 2007).

securing cyberspace.[12] As part of the review, CSIS recommended the creation of a new National Office of Cyberspace, which would work with OSTP to provide overall coordination of cybersecurity R&D.

- The Institute for Information Infrastructure Protection's report, entitled *National Cyber Security: Research and Development Challenges Related to Economics, Physical Infrastructure, and Human Behavior*, stated that a national cybersecurity research agenda was urgently needed that prioritizes problems; encourages and tracks innovative approaches; and provides a pipeline of short-, medium-, and long-term projects.[13]

- The National Security and Homeland Security Councils' report, entitled *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, recommended that a framework for R&D be developed.[14] The report also recommended that the administration appoint a cybersecurity policy official to coordinate the nation's cybersecurity policies and activities. Accordingly, as we have previously mentioned, in December 2009, President Obama appointed a national Cybersecurity Coordinator. Among many things, this official is tasked with updating the national cybersecurity strategy. We have a review under way that is assessing the implementation status of the recommendations that were made in the *Cyberspace Policy Review*.

- In November 2009, DHS issued a report entitled *A Roadmap for Cybersecurity Research*, which identifies critical needs and gaps in 11 cybersecurity research areas.

[12] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cyber Security for the 44th Presidency* (Washington, D.C.: December 2008).

[13] The Institute for Information Infrastructure Protection is a national consortium of academic institutions, federally funded labs, and nonprofit organizations dedicated to strengthening the cyber infrastructure of the United States.

[14] The National Security Council and the Homeland Security Council, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

GAO Has Made Recommendations to Improve Cybersecurity R&D

In addition to the recent cybersecurity reports, we have reported on the importance of furthering cybersecurity R&D. Specifically, in September 2006, we reported on actions taken by federal entities to improve the oversight and coordination of federal cybersecurity R&D activities.[15] We found that federal entities had taken several important steps to improve the oversight and coordination of federal cybersecurity R&D; however, a federal cybersecurity research agenda had not yet been developed. Furthermore, the federal government's R&D repositories did not contain information about all of the federally funded cybersecurity research projects. As a result, we recommended, among other things, that the Director of OSTP establish firm timelines for the completion of the federal cybersecurity R&D agenda, which includes near-term, mid-term, and long-term research. We also recommended that the Director of OMB issue guidance to agencies on reporting information about federally funded cybersecurity R&D projects to the governmentwide repositories. Although OMB and OSTP have taken initial steps, the agencies have not fully implemented these recommendations.

Additionally, in March 2009, we testified on key improvements needed to strengthen the national cybersecurity strategy. Based on input we received from expert panels, we identified 12 key improvements that are essential to enhancing the strategy and our national cybersecurity posture.[16] One of these improvements was placing greater emphasis on cybersecurity R&D, including consideration of how to better coordinate government and private sector efforts.

Key Challenges to Improving National Cybersecurity R&D Efforts

While efforts are under way by OSTP, NITRD, and individual agencies to improve cybersecurity R&D, significant challenges remain. We identified, through input from experts from relevant federal, private, and academic organizations, six major challenges that are impeding efforts to improve cybersecurity R&D.

[15] GAO, *Information Security: Coordination of Federal Cyber Security Research and Development*, GAO-06-811 (Washington, D.C.: Sept. 29, 2006).

[16] GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: Mar. 10, 2009).

Lack of a Prioritized National Cybersecurity R&D Agenda

According to key expert bodies, a national cybersecurity R&D agenda should embody several characteristics. Specifically, according to the *National Strategy to Secure Cyberspace*, a national R&D agenda should include near-term (1 to 3 years), mid-term (3 to 5 years), and long-term (5 years and longer) goals. Additionally, an agenda should include national-level R&D priorities that go beyond goals specific to agencies' and companies' missions. It is also essential that cyberspace security research efforts are ranked across all sectors and funding sources to ensure that national goals are addressed. Additionally, according to the Institute for Information Infrastructure Protection, it is important that an agenda include perspectives from both the public and private sectors. An agenda should also specify timelines and milestones for conducting cybersecurity R&D activities. Moreover, in 2006, we recommended that OSTP develop a federal cybersecurity R&D agenda that includes near-term, mid-term, and long-term research.[17] Additionally, pursuant to the High-Performance Computing Act of 1991, as amended by the Next Generation Internet Research Act of 1998 and the America COMPETES Act of 2007, NITRD is responsible for setting goals and priorities for cybersecurity R&D.

However, despite its legal responsibility and our past recommendations, NITRD has not created a prioritized national or federal R&D agenda. Officials from DOD, DOE, and DHS indicated that there is a lack of a prioritized cybersecurity R&D agenda. Furthermore, the aggregated ranked responses from 24 cybersecurity R&D private and academic experts we contacted indicated that the lack of a prioritized national R&D agenda is the top challenge that they believe should be addressed.[18]

While officials from NITRD and OMB stated that they consider the following key documents to comprise a national R&D agenda, these documents do not constitute, whether taken collectively or separately, a prioritized national agenda:

- NITRD's 2006 Cyber Security and Information Assurance Working Group's *Federal Plan for Cyber Security and Information Assurance R&D*: As we have previously reported, this plan was intended to be the first step toward developing a federal agenda for cybersecurity research, which provides baseline information about ongoing federal R&D activities;

[17] GAO-06-811.

[18] Experts from 3 of the 27 private sector organizations and academic institutions did not respond to our request to rank the challenges.

however, mid-term and long-term cybersecurity research goals were not defined. Furthermore, the plan does not specify timelines and milestones for conducting R&D activities, nor does it assign responsibility for implementation. Additionally, this plan was published in 2006, and many experts indicated that it is outdated. For example, NSF officials, who were co-developers of the plan, stated that the document does not take into account new types of threats that have appeared in the past 4 years, and some of the issues identified in the 2006 report are less critical today. According to NITRD officials, this plan is intended to be a 5-year plan, and they do not plan to update it until 2012.

- The National Security and Homeland Security Councils' 2009 *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*: This report presents relevant high-level challenges and recommendations for improvements that cover the spectrum of cybersecurity issues. However, according to NSF officials, the report does not contain sufficient detail related to R&D to be a research agenda. Furthermore, DHS officials stated that the *Cyberspace Policy Review* does not attempt to articulate a national-level R&D agenda.

- August 2009 OMB and OSTP memorandum, "Science and Technology Priorities for the FY 2011 Budget (M-09-27)": This memorandum also does not provide guidance on cybersecurity R&D priorities. As pointed out by DHS officials, this memorandum provides high-level points for consideration but does not provide a clear national cybersecurity R&D agenda. Moreover, DOD stated that the memorandum only provides general guidance for departments and agencies as they develop their overall science and technology programs.

- National Science and Technology Council's 2008 *Federal Plan for Advanced Networking and Research and Development*: This plan specifically focuses on establishing goals and time frames for enhancing networking capabilities, which includes enhancing networking security and reliability. However, networking is just one of several areas that need to be addressed in the cybersecurity R&D arena.

The private sector organizations and cybersecurity R&D experts that we contacted also did not consider the documents to constitute a national R&D agenda. Several private sector representatives stated that they exclusively use their own strategies to determine their cybersecurity R&D priorities.

According to NITRD's Cyber Security and Information Assurance Interagency Working Group (CSIA IWG) members, they have recently begun working on developing a framework that focuses on three main cybersecurity R&D themes. The DOD co-chair of CSIA IWG stated that he believes the framework will constitute a national cybersecurity R&D agenda. The three themes that comprise the framework are (1) supporting security policies and security services for different types of cyber space interactions; (2) deploying systems that are both diverse and changing, to increase complexity and costs for attackers and system resiliency; and (3) developing cybersecurity incentives to create foundations for cybersecurity markets, establish meaningful metrics, and promote economically sound and secure practices. NITRD officials stated that they expect the framework to be finalized in time for the 2012 budget submission. However, these three themes do not cover all of the priorities that should be included in a national cybersecurity R&D agenda. For example, among other things, issues such as global-scale identity management, which was identified by DHS as a top problem that needs to be addressed, and computer forensics, which was identified by the private sector and several key government reports as a major area needing government focus, are not included in this framework.

Beyond developing a federal plan as we have previously recommended, there is a need for a broader national cybersecurity R&D agenda. Until such an agenda is developed that (1) contains short-term, mid-term, and long-term priorities, (2) includes input from both public and private sectors, and (3) is consistent with the updated national cybersecurity strategy (when it is available), increased risk exists that agencies and private sector organizations will focus on their individual priorities for cybersecurity R&D, which may not be the most important national research priorities.

Lack of Leadership for Improving Federal Cybersecurity R&D Efforts

According to key expert bodies, leadership for improving cybersecurity in R&D is composed of several attributes. Specifically, PITAC indicated that federal cybersecurity R&D efforts should be focused, coordinated, and overseen by a central body. More specifically, the committee recommended that NITRD become the focal point for coordinating federal cybersecurity R&D efforts. Furthermore, according to CSIS, NITRD should lead the nation toward an aggressive research agenda. Additionally, our previous work has highlighted the need to define and agree on roles and responsibilities, including how an effort will be led. In doing so, the entities can clarify who will do what, organize their joint and individual efforts, and facilitate decision making.[19]

Although NITRD is primarily responsible for providing leadership in coordinating cybersecurity R&D, it has played a facilitator role, rather than leading agencies in a strategic direction toward a cybersecurity R&D agenda. Experts from 24 private sector and academic R&D entities ranked this challenge as the second most important cybersecurity R&D challenge, and officials from 2 federal agencies indicated that they agreed that there is a lack of government leadership. For example, 2 private sector experts stated that there is confusion about who in the government is leading the cybersecurity R&D area. Another private sector expert stated that while NITRD is playing a facilitator role, there is no central entity that is strategically leading cybersecurity R&D in the federal government.

NITRD has intentionally decided to play a facilitator role. Specifically, NITRD carries out several activities, such as hosting monthly meetings in which agencies discuss their initiatives and compiling all of its participating agencies' cybersecurity R&D efforts and budgets; however, it generally does not make any specific decisions about how these efforts could be better coordinated. Recently, NITRD pointed to the National Cyber Leap Year initiative and the output from that initiative—CSIA IWG's cybersecurity R&D framework that is under development—as evidence of NITRD's leadership approach; however, this framework has not been completed.

Until NITRD exercises its leadership responsibilities, federal agencies will likely lack overall direction for cybersecurity R&D.

[19] See, for example, GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005); and *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006).

Lack of a Process for Sharing Key Information on R&D Initiatives between Federal Agencies and the Private Sector

We have previously emphasized the importance of establishing a process to ensure widespread and ongoing sharing of key cybersecurity-related information between federal agencies and private sector entities.[20] Additionally, according to the 2009 *Cyberspace Policy Review*, it is important that the federal government share cybersecurity R&D information with the private sector.

To improve R&D-related information sharing, in 2008 the Information Technology Sector Coordinating Council (IT-SCC) R&D working group proposed a framework to the Information Technology Government Coordinating Council and NITRD to establish a process for federal agencies and the private sector to share key information on R&D initiatives.[21] Approximately 2 years have passed since the IT-SCC made its proposal, and still no decision has been made on whether the government will pursue the working group's proposal, nor has the government developed an alternative approach to sharing key R&D information.

According to federal and private experts, key factors exist that reduce the private sector's and government's willingness to share information and trust each other with regard to researching and developing new cybersecurity technologies. Specifically, private sector officials stated that they are often unwilling to share details of their R&D with the government because they want to protect their intellectual property. On the government side, officials are concerned that the private sector is too focused on making a profit and may not necessarily conduct R&D in areas

[20] For more information on GAO reports and recommendations related to information sharing, see GAO, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001); *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, D.C.: July 09, 2004); *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005); *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005); and *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C.: July 31, 2008).

[21] The IT-SCC R&D working group's proposal consists of establishing a repeatable process in which the private sector and government would, among other things, identify gaps between R&D initiatives and priorities in the public and private sectors. The gap analysis would be developed by both sectors sharing their current R&D activities; infrastructure risks, threats, and vulnerabilities; and known conditions (e.g., integrity of software code and pieces of the infrastructure that are not inherently secure). It was proposed that this work would result in a published document that would articulate R&D priorities and a roadmap and would be updated on a regular basis.

that require the most attention. Additionally, government and private sector officials indicated that the government does not have a process in place to communicate the results on completed federal R&D.

The private and public sectors share some cybersecurity R&D information, but such information-sharing generally occurs only on a project-by-project basis. For example, NSF's Industry University Cooperative Research Center initiative establishes centers to conduct research that is of interest to both industry and academia, and DOD's Small Business Innovation Research program funds R&D at small technology companies. However, according to federal and private sector experts, widespread and ongoing information-sharing generally does not occur. Without sharing such information, gaps in research among public and private sectors R&D is difficult to identify.

More recently, NITRD has taken steps to work more formally with the private sector and academia, such as hosting the National Cyber Leap Year Summit in August 2009, which aimed to bring together researchers and developers from the private and public sectors.

Nevertheless, without an ongoing process for industry and government to share cybersecurity R&D information, the nation could be at great risk of funding duplicative efforts or having gaps in needed R&D.

Limited Focus on Long-term, Complex Cybersecurity Research Projects

Several entities have emphasized that cybersecurity R&D should include long-term, complex projects. Specifically, the President's 2003 National Strategy to Secure Cyberspace indicated that it is important that the Director of OSTP develop a cybersecurity research agenda that includes long-term (5 years and longer) research. In 2006, we reported that researchers had indicated the need for long-term efforts, such as researching cybersecurity vulnerabilities, developing technological solutions, and transitioning research results into commercially available products.[22] Furthermore, in August 2007, PCAST recommended that federal agencies increase support for larger-scale, longer-term R&D.

[22] GAO-06-811.

While federal officials point to specific long-term cybersecurity R&D investments, such as DOD's development of a National Cyber Range[23] and NSF's Trustworthy Computing Program, OSTP has not established long-term research goals in a national agenda, the absence of which continues to plague the advancement of cybersecurity R&D. According to experts, one of the contributing factors to the limited focus on long-term R&D is that industry is focused on short-term, profit-generating R&D. Furthermore, experts stated that unless there is commercial viability, industry generally does not invest time or money. Another major contributing factor is that the federal government has been focused on obtaining and implementing new solutions immediately. For example, federal cybersecurity grants generally require grantees to deliver their research within a 3 year period, and, according to a cybersecurity expert at Purdue University, in many cases grantees are required to show the progress of their research within 6 months.

Although highly beneficial, short-term R&D, by definition, has limited focus and is not intended to independently tackle the more complex and fundamental problems related to cybersecurity, such as security problems related to the Internet's infrastructure. If the focus on cybersecurity R&D continues to be short-term and confined to our current technological environment, it may result in stunted research and growth, short-term fixes for systems, and networks that may not necessarily be developed with the most appropriate security.

Lack of a Sufficient Information Technology Human Capital Skill Base

Legislation and several key reports have stressed the importance of having sufficient cybersecurity education programs and an ample supply of qualified cybersecurity professionals. Specifically, the Cyber Security Research and Development Act stated that the United States needs to expand and improve the pool of information security professionals, including researchers, in the workforce.[24] In addition, the INFOSEC

[23] DOD's National Cyber Range is a testing environment for cybersecurity researchers to assist in producing qualitative and quantitative assessments of various cybersecurity technologies and scenarios. This was developed under CNCI.

[24] 15 U.S.C. § 7401(5)(B).

Research Council[25] reported that it is important that the United States enhance cybersecurity academic education and training.[26] In December 2008, the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency reported that the federal government needs to increase the supply of skilled workers and to create a career path (including training and advancement) for cyberspace specialists in the federal government.[27] Furthermore, one of the national Cybersecurity Coordinator's responsibilities is updating the national cybersecurity strategy, which addresses the cybersecurity human capital needs, among other things.

While several federal programs intended to promote cybersecurity-related professions exist today—such as NSF's Pathways to Revitalize Undergraduate Computing Education program and DOD's Science, Mathematics and Research for Transformation Scholarship for Service program, which seek to develop a U.S. workforce with computing competencies—government officials and private sector experts agree that more can be done. For example, DHS officials indicated there is a shortage of cybersecurity R&D management officials. DOD officials indicated that more can be done to encourage personnel to pursue security degrees, and officials from DOE stated that it is very difficult to find highly qualified researchers with the requisite experience. Private sector experts voiced similar concerns, such as the need to cultivate talented people and the need for employees with more cybersecurity R&D experience.

Government officials and cybersecurity experts suggested that several factors have contributed to the lack of human capital expertise in the area of cybersecurity R&D. For example, federal officials and cybersecurity experts suggested that unclear career paths in cybersecurity have contributed to the lack of a sufficient skill base. Another expert stated that colleges or universities do not have the appropriate tools and products to adequately teach cybersecurity to students. While it has been 7 years since

[25] The INFOSEC Research Council consists of government sponsors of information security research from DOD, the intelligence community, and federal civil agencies. The council aims to provide its membership with a communitywide forum to discuss critical information security issues, convey the research needs of their respective communities, and describe current research initiatives and proposed courses of action for future research investments.

[26] INFOSEC Research Council, *Hard Problems List* (November 2005).

[27] *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission.*

The National Strategy to Secure Cyberspace articulated plans for improving training and creating certifications, human capital weaknesses still exist.

Without obtaining information on the shortages in researchers in the cybersecurity field, it will be difficult for the national Cybersecurity Coordinator to update the national cybersecurity strategy with the appropriate cybersecurity human capital plans for addressing such weaknesses.

No Mechanism in Place That Identifies All Cybersecurity R&D Initiatives and Funding

Congress has recognized the importance of making available information on federal R&D funding for coordinating federal research activities and improving collaboration among those conducting federal R&D. To improve the methods by which government information is organized, preserved, and made accessible to the public, the E-Government Act of 2002 mandated that OMB ensure the development and maintenance of a governmentwide repository and Web site that integrates information about federally funded R&D, including R&D related to cybersecurity.[28] The Director of OMB delegated this responsibility to NSF.

As we have previously reported, NSF maintained a repository for federally funded R&D, known as the Research and Development in the U.S. (RaDiUS) database; however, the database was incomplete and not fully populated.[29] Therefore, in 2006, we recommended that OMB issue guidance to agencies on reporting information about federally funded cybersecurity R&D projects to RaDiUS. OMB did not implement our recommendation. In 2008, the database was decommissioned because, according to a senior official at NSF, the data were incomplete, users had difficulty using it, and the database was built with antiquated technology. In March 2010, OMB officials stated that they are currently evaluating several repositories to replace RaDiUS as a centralized database to house all government-funded R&D programs, including cybersecurity R&D. While officials stated that they anticipate making a decision on a database by the end of fiscal year 2010, officials were unable to specify when a database would be in place that tracks all cybersecurity R&D information. Additionally, it is not clear how this fits into the overall coordination efforts for which NITRD is responsible.

[28] Pub. L. No. 107-347, § 207(g)(1)(A), 116 Stat. 2899, 2919-21 (Dec. 17, 2002).

[29] GAO-06-811.

Tracking funding that is allocated to classified R&D adds to the complexity of this challenge. For example, according to a DOD official, the majority of DOD's cybersecurity R&D is composed of either classified R&D or unclassified components of a program mixed with classified components, thereby rendering the entire program as classified. As such, it is difficult to identify the exact funding that is allocated to classified versus unclassified R&D.

There is currently no mechanism in place that identifies all cybersecurity R&D initiatives governmentwide and associated funding. DHS officials stated that it would be helpful to have a clearinghouse that they could use to view what activities are already being conducted by the government. In addition, a private sector expert stated that having a centralized database in place would improve coordination between the public and private sectors. However, challenges to maintaining such a mechanism exist. For example, an OSTP official indicated that it is difficult to develop and enforce policies for identifying specific funding as R&D. Additionally, the level of detail to be disclosed is also a factor because national security must also be protected.

However, without a mechanism to track all active and completed cybersecurity R&D initiatives, federal researchers and developers as well as private companies lack essential information about ongoing and completed R&D, thus increasing the likelihood of duplicative efforts, inefficient use of government funding, and lost collaboration opportunities. Additionally, without a complete understanding of how much each federal agency is spending on cybersecurity R&D, it may be difficult to make the appropriate resource allocation decisions.

Conclusions

OSTP and NITRD have recently taken steps to try to improve the coordination and oversight of cybersecurity R&D. However, key challenges still exist, and, until these challenges are addressed, the United States may continue to struggle in protecting and securing its critical systems and networks. Specifically, the absence of a national cybersecurity R&D agenda and leadership increases the risk that efforts will not reflect national priorities, key decisions will be postponed, and federal agencies will lack overall direction for their efforts. Furthermore, without sufficient attention to complex, long-term research projects and input on the current weaknesses and shortages in researchers in cybersecurity, the nation risks falling behind in cybersecurity and not being able to adequately protect its digital infrastructure. Finally, the lack of a mechanism to track all active and completed cybersecurity R&D

initiatives and the lack of a process for sharing information among the public and private sectors may result in duplicative efforts or gaps in needed R&D.

Recommendation for Executive Action

To help address the key cybersecurity R&D challenges, we are recommending that the Director of the Office of Science and Technology Policy, in conjunction with the national Cybersecurity Coordinator, direct the Subcommittee on Networking and Information Technology Research and Development to exercise its leadership responsibilities and take the following four actions:

- Establish a comprehensive national R&D agenda by expanding on the CSIA IWG framework and ensure that it
  - contains priorities for short-term, mid-term, and long-term complex cybersecurity R&D;
  - includes input from the private sector and academia; and
  - is consistent with the updated national cybersecurity strategy (when available).
- Identify and report shortages in researchers in the cybersecurity field to the national Cybersecurity Coordinator, which should be used to update the national cybersecurity strategy with the appropriate plans for addressing human capital weaknesses.
- Establish a mechanism, in working with the Office of Management and Budget and consistent with existing law, to keep track of all ongoing and completed federal cybersecurity R&D projects and associated funding, to the maximum extent possible without jeopardizing national security.
- Utilize the newly established tracking mechanism to develop an ongoing process to make federal R&D information available to federal agencies and the private sector.

Agency Comments and Our Evaluation

We received written comments on a draft of this report, which were transmitted via e-mail by OSTP's Assistant Director for Information Technology R&D. We also received written comments from the Director of NIST. Letters from these agencies are reprinted in appendixes II and III. In addition, we received comments from a Senior Science Advisor from NSF and technical comments from the Director of the Departmental Audit

Liaison from DHS, via e-mail. Additionally, representatives from DOE indicated via e-mail that they reviewed the draft report and did not have any comments. Officials from DOD and OMB did not respond to our request for comments.

The Assistant Director for Information Technology R&D from OSTP agreed with our recommendation and provided details on the office's plans and actions to address our recommendation. For example, to address the part of the recommendation to establish a comprehensive national R&D agenda, OSTP has begun updating its current 5-year plan for cybersecurity R&D. Additionally, to address the portion of the recommendation to identify and report shortages in researchers in the cybersecurity field, NITRD officials plan to provide an assessment of these shortages as part of their annual planning and review processes. The Assistant Director for Information Technology R&D also indicated that OSTP did not concur with certain findings within our report; however, he did not provide any additional information.

The Director of NIST indicated that he agreed with our recommendation. However, he stated NIST officials recommended that we make two changes to the draft report. First, the officials believe that OSTP and NITRD are coordinating research activities and working with the federal government research community to identify a research strategy that meets critical future needs in cybersecurity. We acknowledge in the report that NITRD facilitates several activities, such as hosting monthly meetings in which agencies discuss their initiatives and compiling all of its participating agencies' cybersecurity R&D efforts and budgets. We also acknowledge that NITRD hosted the National Cyber Leap Year Summit in August 2009, which aimed to bring together researchers and developers from the private and public sectors. Nevertheless, as we state in the report, NITRD is not leading agencies in a strategic direction toward a cybersecurity agenda. Second, officials requested that we add a sentence that officials from NIST believe that a prioritized research strategy is evolving and agencies will base their research agenda on this strategy and their mission needs. We acknowledge in the report that NITRD is currently working on developing a framework that focuses on three main cybersecurity R&D themes. NITRD officials expect the framework to be finalized in time for the 2012 budget submission. However, these themes do not cover all of the priorities that should be included in a national cybersecurity R&D agenda.

Regarding comments from NSF's Senior Science Advisor, she indicated that she generally agreed with our recommendation. The Senior Science

Advisor and the Departmental Audit Liaison from DHS provided technical comments, which have been incorporated in the report where appropriate.

As arranged with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will be sending copies of this report to interested congressional committees; the Secretaries of Homeland Security, Defense, Energy, and Commerce; the Directors of the Office of Science and Technology Policy, Office of Management and Budget, and National Science Foundation; and other interested parties. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staffs have any questions on the matters discussed in this report, please contact David A. Powner at (202) 512-9286 or powned@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

David A. Pow

David A. Powner
Director, Information Technology
Management Issues

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objective, Scope, and Methodology

The objective of our review was to determine the key challenges to enhancing national-level cybersecurity research and development (R&D) efforts among the federal government and private companies.

To identify the key agencies involved in federal cybersecurity R&D, we researched several cybersecurity R&D-related documents, including the President's Information Technology Advisory Committee 2005 report, the Subcommittee on Networking and Information Technology Research and Development's (NITRD) Cyber Security and Information Assurance Working Group's *2006 Federal Plan for Cyber Security and Information Assurance R&D*, the Institute for Information Infrastructure Protection 2009 Report, and the National Security and Homeland Security Councils' *Cyberspace Policy Review*. We also reviewed NITRD's *2010 Supplement to the President's Budget*, which lists key agencies that fund and conduct cybersecurity R&D, and a previous GAO report[1] to identify the agencies that provide high-level oversight. These agencies include the Departments of Defense, Energy, and Homeland Security; the National Institute of Standards and Technology; the National Science Foundation; the Office of Management and Budget; and the Office of Science and Technology Policy.

To identify private sector organizations with a major role in cybersecurity R&D, we consulted and interviewed cybersecurity experts in the information technology (IT) and communication sectors. We developed a list of companies through the membership lists of IT and communication private sector councils, which are composed of a wide range of companies that specialize in these areas. We narrowed down the list by asking each company whether they conduct cybersecurity R&D and whether they would be willing to speak to us about their cybersecurity R&D priorities, as well as their views on what role the government should be playing in the cybersecurity R&D arena. Those that responded positively to our questions consisted of 18 companies that we included in our review. We also identified 9 additional private sector and academic organizations. We selected these experts on the basis of those we have consulted in previous reviews or who were recommended to us by other experts. Additionally, we identified other academic experts from our Executive Council for Information Management and Technology, which is composed of public- and private-sector IT management experts who assist us in obtaining

[1] GAO, *Information Security: Coordination of Federal Cyber Security Research and Development*, GAO-06-811 (Washington, D.C.: Sept. 29, 2006).

different perspectives on current IT management and policy issues. We included the following industry and academic entities in our review:

Alcatel-Lucent
AT&T
Carnegie Mellon University
Digital Intelligence
Google
IBM Corporation
Information Security Forum
Information Technology Sector Coordinating Council
In-Q-Tel
Intel Corporation
Lumeta Corporation
McAfee, Inc.
Microsoft
Net Witness
Neustar
Purdue University
Oracle Corporation
Raytheon BBN Technologies
Renesys
StrongAuth, Inc.
Symantec
University at Albany, Center for Technology in Government
Verizon Business

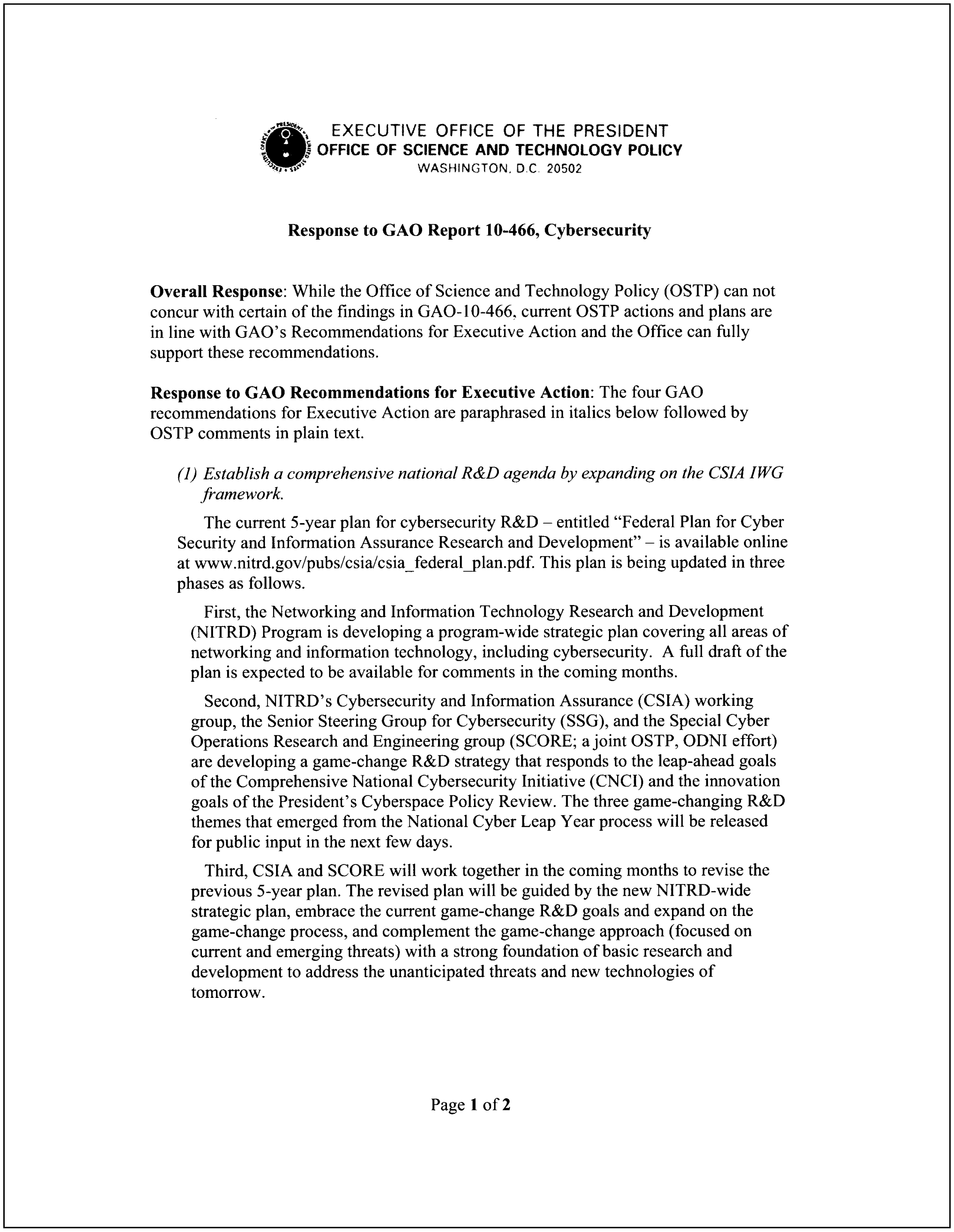
Three of the 27 academic and private organizations asked us not to include their names in our report, and one expert was a private sector consultant who was a former director of the National Coordination Office.

To identify key challenges to enhancing national-level cybersecurity R&D efforts, we analyzed documentation, such as agencies' research plans and cybersecurity reports, and interviewed federal officials and industry experts. We then aggregated the identified challenges and validated the top challenges by asking the experts to rank the challenges in order of importance.

In addition, we analyzed relevant federal law and policy, including the National Strategy to Secure Cyberspace, the High-Performance Computing Act of 1991, the E-Government Act of 2002, the Cyber Security Research and Development Act, the Next Generation Internet Research Act of 1998, and Homeland Security Presidential Directive 7. We also reviewed prior GAO reports.

We conducted this performance audit from June 2009 to June 2010, 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Office of Science and Technology Policy



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

Response to GAO Report 10-466, Cybersecurity

Overall Response: While the Office of Science and Technology Policy (OSTP) can not concur with certain of the findings in GAO-10-466, current OSTP actions and plans are in line with GAO's Recommendations for Executive Action and the Office can fully support these recommendations.

Response to GAO Recommendations for Executive Action: The four GAO recommendations for Executive Action are paraphrased in italics below followed by OSTP comments in plain text.

(1) *Establish a comprehensive national R&D agenda by expanding on the CSIA IWG framework.*

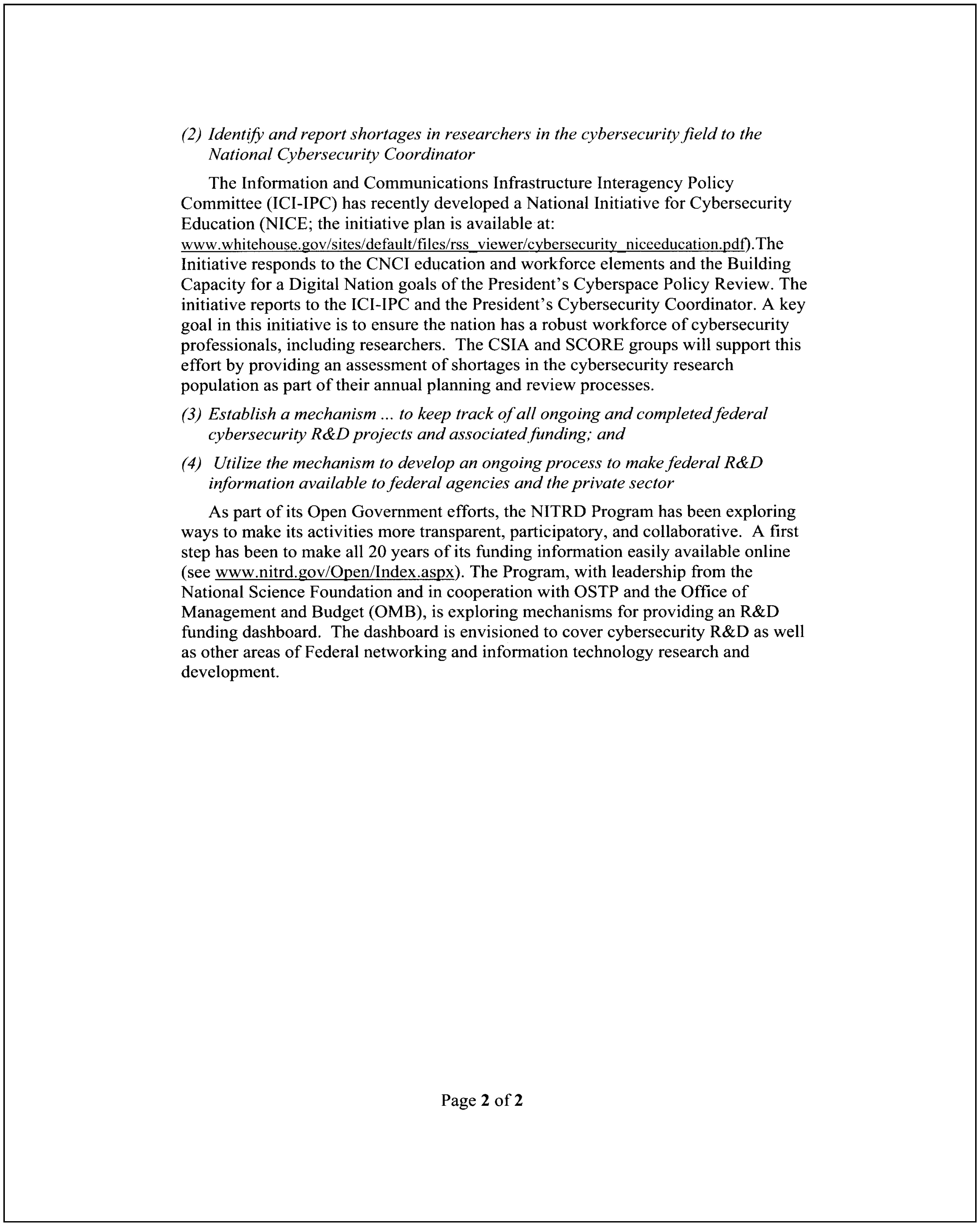
The current 5-year plan for cybersecurity R&D – entitled "Federal Plan for Cyber Security and Information Assurance Research and Development" – is available online at www.nitrd.gov/pubs/csia/csia_federal_plan.pdf. This plan is being updated in three phases as follows.

First, the Networking and Information Technology Research and Development (NITRD) Program is developing a program-wide strategic plan covering all areas of networking and information technology, including cybersecurity. A full draft of the plan is expected to be available for comments in the coming months.

Second, NITRD's Cybersecurity and Information Assurance (CSIA) working group, the Senior Steering Group for Cybersecurity (SSG), and the Special Cyber Operations Research and Engineering group (SCORE; a joint OSTP, ODNI effort) are developing a game-change R&D strategy that responds to the leap-ahead goals of the Comprehensive National Cybersecurity Initiative (CNCI) and the innovation goals of the President's Cyberspace Policy Review. The three game-changing R&D themes that emerged from the National Cyber Leap Year process will be released for public input in the next few days.

Third, CSIA and SCORE will work together in the coming months to revise the previous 5-year plan. The revised plan will be guided by the new NITRD-wide strategic plan, embrace the current game-change R&D goals and expand on the game-change process, and complement the game-change approach (focused on current and emerging threats) with a strong foundation of basic research and development to address the unanticipated threats and new technologies of tomorrow.

Page **1** of **2**



(2) Identify and report shortages in researchers in the cybersecurity field to the National Cybersecurity Coordinator

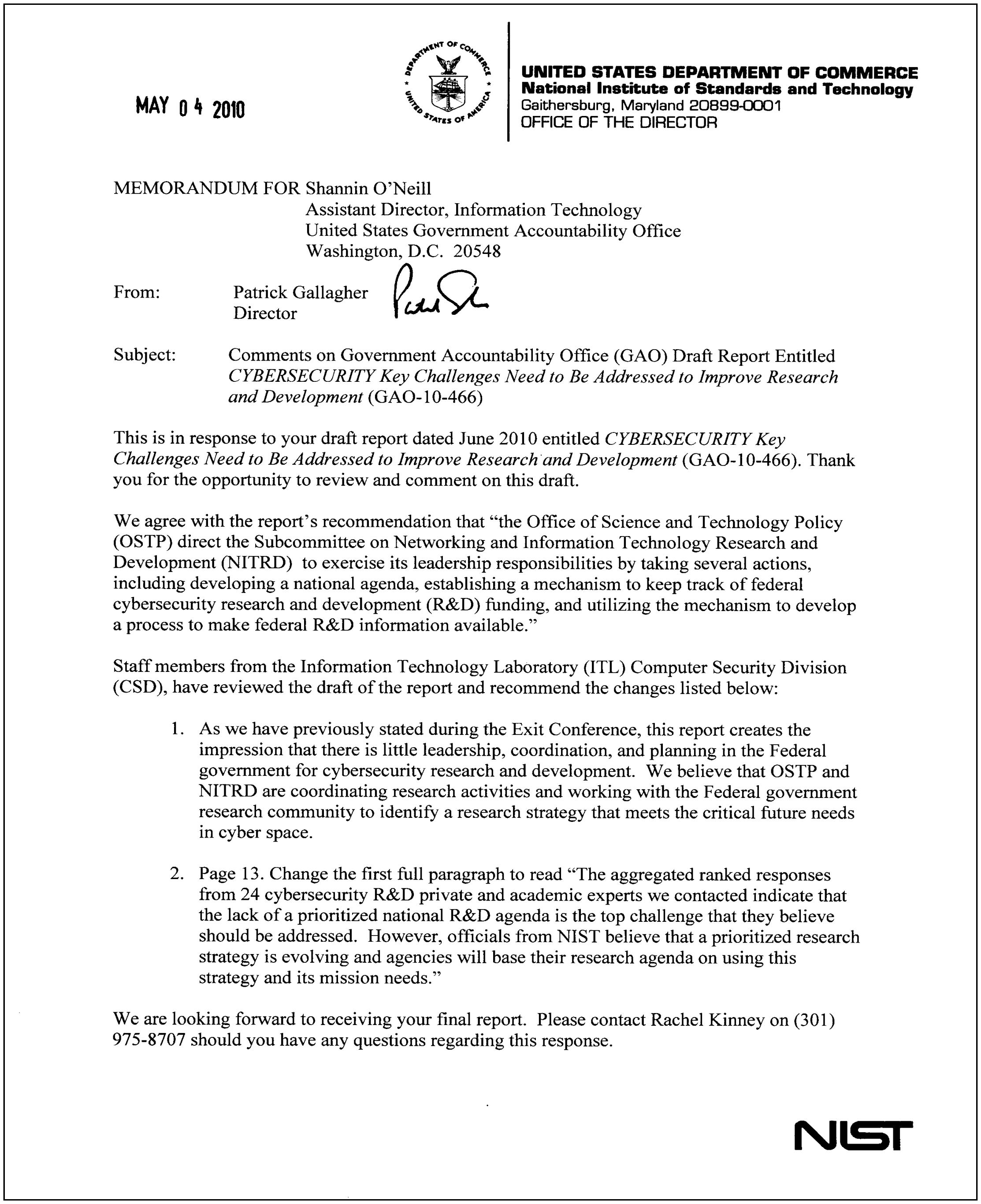
The Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC) has recently developed a National Initiative for Cybersecurity Education (NICE; the initiative plan is available at: www.whitehouse.gov/sites/default/files/rss_viewer/cybersecurity_niceeducation.pdf).The Initiative responds to the CNCI education and workforce elements and the Building Capacity for a Digital Nation goals of the President's Cyberspace Policy Review. The initiative reports to the ICI-IPC and the President's Cybersecurity Coordinator. A key goal in this initiative is to ensure the nation has a robust workforce of cybersecurity professionals, including researchers. The CSIA and SCORE groups will support this effort by providing an assessment of shortages in the cybersecurity research population as part of their annual planning and review processes.

(3) Establish a mechanism ... to keep track of all ongoing and completed federal cybersecurity R&D projects and associated funding; and

(4) Utilize the mechanism to develop an ongoing process to make federal R&D information available to federal agencies and the private sector

As part of its Open Government efforts, the NITRD Program has been exploring ways to make its activities more transparent, participatory, and collaborative. A first step has been to make all 20 years of its funding information easily available online (see www.nitrd.gov/Open/Index.aspx). The Program, with leadership from the National Science Foundation and in cooperation with OSTP and the Office of Management and Budget (OMB), is exploring mechanisms for providing an R&D funding dashboard. The dashboard is envisioned to cover cybersecurity R&D as well as other areas of Federal networking and information technology research and development.

Appendix III: Comments from the National Institute of Standards and Technology



MAY 04 2010

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-0001
OFFICE OF THE DIRECTOR

MEMORANDUM FOR Shannin O'Neill
Assistant Director, Information Technology
United States Government Accountability Office
Washington, D.C. 20548

From: Patrick Gallagher
Director

Subject: Comments on Government Accountability Office (GAO) Draft Report Entitled *CYBERSECURITY Key Challenges Need to Be Addressed to Improve Research and Development* (GAO-10-466)

This is in response to your draft report dated June 2010 entitled *CYBERSECURITY Key Challenges Need to Be Addressed to Improve Research and Development* (GAO-10-466). Thank you for the opportunity to review and comment on this draft.

We agree with the report's recommendation that "the Office of Science and Technology Policy (OSTP) direct the Subcommittee on Networking and Information Technology Research and Development (NITRD) to exercise its leadership responsibilities by taking several actions, including developing a national agenda, establishing a mechanism to keep track of federal cybersecurity research and development (R&D) funding, and utilizing the mechanism to develop a process to make federal R&D information available."

Staff members from the Information Technology Laboratory (ITL) Computer Security Division (CSD), have reviewed the draft of the report and recommend the changes listed below:

1. As we have previously stated during the Exit Conference, this report creates the impression that there is little leadership, coordination, and planning in the Federal government for cybersecurity research and development. We believe that OSTP and NITRD are coordinating research activities and working with the Federal government research community to identify a research strategy that meets the critical future needs in cyber space.

2. Page 13. Change the first full paragraph to read "The aggregated ranked responses from 24 cybersecurity R&D private and academic experts we contacted indicate that the lack of a prioritized national R&D agenda is the top challenge that they believe should be addressed. However, officials from NIST believe that a prioritized research strategy is evolving and agencies will base their research agenda on using this strategy and its mission needs."

We are looking forward to receiving your final report. Please contact Rachel Kinney on (301) 975-8707 should you have any questions regarding this response.

NIST

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

David A. Powner at (202) 512-9286 or pownerd@gao.gov
Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contacts named above, the following staff also made key contributions to this report: Shannin O'Neill, Assistant Director; Rebecca Alvarez; Jamey Collins; Eric Costello; Min Hyun; Sairah Ijaz; Kendrick Johnson; Anjalique Lawrence; Lee McCracken; and Kevin Walsh.

(311208)

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