United States Government Accountability Office

GAO

Report to the Chairman, Committee on Government Reform, House of Representatives

September 2006

INFORMATION SECURITY

Coordination of Federal Cyber Security Research and Development

GAO-06-811

September 2006

INFORMATION SECURITY

Coordination of Federal Cyber Security Research and Development

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-811, a report to Chairman, Committee on Government Reform, House of Representatives

Why GAO Did This Study

Research and development (R&D) of cyber security 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. The *National Strategy to Secure Cyberspace* identifies national priorities to secure cyberspace, including a federal R&D agenda.

GAO was asked to identify the (1) federal entities involved in cyber security R&D; (2) actions taken to improve oversight and coordination of federal cyber security R&D, including developing a federal research agenda; and (3) methods used for technology transfer at agencies with significant activities in this area. To do this, GAO examined relevant laws, policies, budget documents, plans, and reports.

What GAO Recommends

GAO recommends that the Office of Science and Technology Policy establish timelines for developing a federal agenda for cyber security research. GAO also recommends that the Office of Management and Budget (OMB) issue guidance to agencies for providing cyber security research data to repositories. In commenting on a draft of this report, OMB stated that it would review the need for such guidance.

www.gao.gov/cgi-bin/getrpt?GAO-06-811.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512.6244 or wilshuseng@gao.gov.

What GAO Found

Several federal entities are involved in federal cyber security research and development. The Office of Science and Technology Policy and OMB establish high-level research priorities. The Office of Science and Technology Policy is to coordinate the development of a federal research agenda for cyber security and oversee the National Science and Technology Council, which prepares R&D strategies that are to be coordinated across federal agencies. The Council operates through its committees, subcommittees, and interagency working groups, which oversee and coordinate activities related to specific science and technology disciplines. The Subcommittee on Networking and Information Technology Research and Development and the Cyber Security and Information Assurance Interagency Working Group are prominently involved in the coordination of cyber security research. In addition, other groups provide mechanisms for coordination of R&D efforts on an informal basis. The National Science Foundation and the Departments of Defense and Homeland Security fund much of this research.

Federal entities have taken several important steps to improve the oversight and coordination of federal cyber security R&D, although limitations remain. Actions taken include chartering an interagency working group to focus on cyber security research, publishing a federal plan for guiding this research, reporting budget information for this research separately, and maintaining repositories of information on R&D projects. However, a federal cyber security research agenda has not been developed as recommended in the *National Strategy to Secure Cyberspace* and the federal plan did not fully address certain key elements. Further, the repositories do not contain information about all of the federally funded cyber security research projects in part because OMB had not issued guidance to ensure that agencies provided all information required for the repositories. As a result, information needed for oversight and coordination of cyber security research activities was not readily available.

Federal agencies use a variety of methods for sharing the results of cyber security research with federal and private organizations (technology transfer), including sharing information through agency Web sites. Other methods include relying on the researcher to disseminate information about his or her research, attending conferences and workshops, working with industry to share information about emerging threats and research, and publishing journals to help facilitate information sharing.

Contents

Abbreviations

CERT/CC	CERT® Coordination Center
OMB	Office of Management and Budget
NITRD	Networking and Information Technology Research and Development
R&D	research and development
RaDiUS	Research and Development in the United States

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 29, 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. However, computers, networks, and their infrastructures were not always designed with security in mind. As a result, these systems 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, protecting both the public and private systems that support critical operations and infrastructures of the federal government has never been more important. Federal law and policy call for critical infrastructure protection activities to enhance the cyber[2] and physical security of the infrastructures that are essential to national security, national economic security, and national public health and safety. These activities include building public-private partnerships, identifying critical infrastructure sectors, identifying federal agencies to work with the sectors to coordinate efforts to strengthen the security of critical infrastructures, and research and development (R&D) of cyber security tools and techniques. Research

[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.

[2]Cyber security refers to the defense against attacks on the information technology infrastructure of an organization, or, in this case, of the federal government and agencies. Cyber security 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. Cyber security is a major concern of both the federal government and the private sector.

in cyber security 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. In this regard, the National Strategy to Secure Cyberspace recommends the development of an annual federal government cyber security research agenda.

In response to your request, our objectives were to identify the

- federal agencies involved in cyber security R&D;
- actions taken to improve oversight and coordination of cyber security R&D, including the development of a federal research agenda; and
- methods used for technology transfer at the agencies with significant activities in cyber security R&D.

To address these objectives, we researched key reports by federal groups on cyber security R&D to determine which agencies are involved in federal cyber security R&D. We identified and interviewed officials at agencies that provide funding for cyber security R&D to determine their decision-making processes, examined policies and procedures, analyzed budget documentation, and determined the extent to which the agencies coordinate their activities. We conducted our work from August 2005 through August 2006 in accordance with generally accepted government auditing standards. Appendix I contains additional details on the objectives, scope, and methodology of our review.

Results in Brief

Numerous entities are involved in federal cyber security research and development. The Office of Science and Technology Policy and Office of Management and Budget (OMB) in the Executive Office of the President provide high-level oversight for federal research and development, including cyber security. The Office of Science and Technology Policy coordinates the development of a federal agenda for cyber security research and oversees the National Science and Technology Council, which prepares R&D strategies that are to be coordinated across federal agencies. The council operates through its committees, subcommittees, and interagency working groups, which oversee and coordinate activities related to specific science and technology disciplines. The Subcommittee on Networking and Information Technology Research and Development (NITRD) and the Interagency Working Group on Cyber Security and Information Assurance are key entities responsible for coordinating federal cyber security R&D activities. In addition, other groups provide

mechanisms for coordination of R&D efforts on an informal basis. Much of the government's cyber security R&D activities are funded or conducted by the National Science Foundation and the Departments of Defense and Homeland Security. Other agencies that also fund or conduct cyber security R&D activities include the Department of Energy, the National Institute of Standards and Technology, and agencies within the intelligence community.

Federal entities have taken several important steps to improve the oversight and coordination of federal cyber security R&D, although limitations remain. Actions taken to facilitate oversight and coordination of cyber security research include (1) chartering an interagency working group to focus on this type of research, (2) publishing a federal plan for cyber security and information assurance that is to provide baseline information and a framework for planning and conducting this research, (3) reporting budget information for cyber security research separately from other types of research, and (4) developing and maintaining governmentwide repositories of information on R&D projects. However, a federal cyber security research agenda has not been developed, as recommended in the National Strategy to Secure Cyberspace and the federal plan does not fully address certain key elements. Further, the governmentwide repositories are incomplete and not fully populated, in part, because OMB has not issued guidance to ensure that agencies provide all information required for the repositories. As a result, key information needed for the effective oversight and coordination of cyber security research activities is not readily available.

The three primary agencies that fund or conduct cyber security R&D use a variety of methods for sharing the results of the research (technology transfer). These methods include relying on the researcher to disseminate information about his or her research, attending conferences and workshops and working with industry to share information about emerging threats and research, and using published peer review journals to facilitate information sharing.

We are recommending that the Director, Office of Science and Technology Policy, establish firm timelines for the completion of the federal cyber security R&D agenda. We are also recommending that the Director, OMB, issue guidance to agencies on reporting information about federally funded cyber security research projects to the governmentwide repositories. The Office of Science and Technology Policy provided technical comments on a draft of this report, but did not comment on our recommendation. We also received oral comments on a draft of our report

from officials at OMB. They stated that they would review the need for issuing guidance. The National Science Foundation and the National Institute of Standards and Technology also provided technical comments, which we have incorporated into the report as appropriate.

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 inexpensively 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.

In a May 2004 report,[3] we discussed how cyber security technologies can provide a near-term solution for improving critical infrastructure security vulnerabilities. However, these technologies offer only single-point solutions by addressing individual vulnerabilities; they do not provide a complete solution. For example, firewalls can control the flow of traffic between networks but cannot protect against threats from within the network; antivirus software can provide some protection against viruses and worms but cannot protect the confidentiality of the data residing on the system. As a result, many researchers have described the use of these types of near-term solutions as being short-sighted. They argue that it is necessary to design systems with built-in security because it is difficult to deploy secure systems based on insecure components. In addition, researchers have indicated that long-term efforts are needed, such as researching cyber security vulnerabilities, developing technological solutions, and transitioning research results into commercially available products. Research in cyber security technology can help create a broader range of choices and more robust tools for building secure, networked computer systems.

[3]GAO, *Technology Assessment: Cyber Security for Critical Infrastructure Protection*, GAO-04-321 (Washington, D.C.: May 28, 2004).

Recent cyber attacks and threats have underscored the need to strengthen and coordinate the federal government's cyber security R&D efforts. Examples of recent attacks include the following:

- In November 2005, the U.S. government issued a warning about a virus disguised in an e-mail purportedly sent from the Federal Bureau of Investigation. The e-mail tells users that they have been visiting illegal Web sites and directs them to open an attachment with a questionnaire that contains a variant of the w32/sober virus. If the attachment is opened, the virus is executed.

- In October 2005, information security specialists reported that the Zotob worm, which had adversely affected computer networks in mid-August, had cost infected organizations an average of $97,000. Variants of the worm were capable of attacks that included logging keystrokes, stealing authentication credentials, and performing mass mailings. It was estimated that it took 61 percent of the impacted organizations more than 80 hours of work to clean up the infected systems.

- In March 2005, security consultants within the electric industry reported that hackers were targeting the U.S. electric power grid and had gained access to electronic control systems. Computer security specialists reported that, in a few cases, these intrusions had "caused an impact." While officials stated that hackers had not caused serious damage to the systems that feed the nation's power grid, the constant threat of intrusion has heightened concerns that electric companies may not have adequately fortified defenses against a potential catastrophic strike.

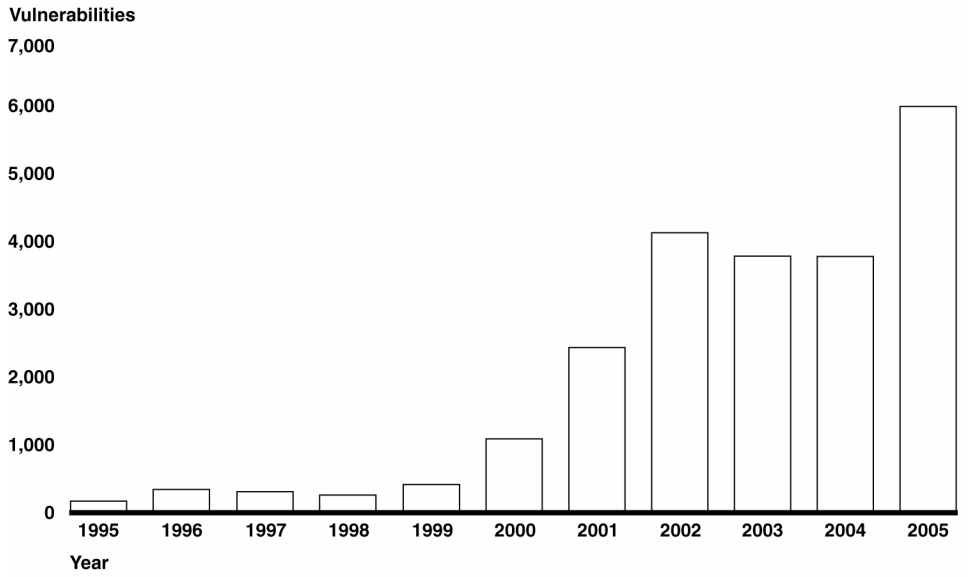
- In January 2005, a major university reported that a hacker had broken into a database containing 32,000 student and employee social security numbers, potentially compromising the identities and finances of the individuals. In similar incidents during 2003 and 2004, it was reported that hackers had attacked the systems of other universities, exposing the personal information of more than 1.8 million people.

The number of malicious attacks has increased with the growing number of vulnerabilities. In 2000, the Software Engineering Institute's CERT® Coordination Center (CERT/CC)[4] received 1,090 reports of security

[4]The CERT®/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

vulnerabilities. By 2005, this number had more than quadrupled to 5,990. Figure 1 illustrates the number of security vulnerabilities reported from 1995 through 2005.

Figure 1: Security Vulnerabilities, 1995–2005



Source: GAO analysis based on CERT/CC data.

Over the years, the federal government has taken these and other actions to improve cyber security efforts:

- publishing best practices and guidelines that assist in the planning, selection, and implementation of cyber security technologies;
- partnering with private sector counterparts to assess vulnerabilities and develop plans to eliminate those vulnerabilities; and
- awarding grants to support cyber security R&D.

Federal Cyber Security Research and Development Policies

Research associated with enhancing the cyber security of critical infrastructures has been reinforced through federal requirements aimed at improving the nation's cyber security posture. Additional requirements for research can be found in legislation that establishes agency responsibilities. For example, the act that establishes the Office of Science and Technology Policy gives the office the responsibility of assisting the

President in providing general leadership and coordination of the research programs of the federal government.[5] To provide a historical perspective, table 1 summarizes the key federal cyber security R&D actions that have shaped the development of the federal government's cyber security R&D policies.

Table 1: Key Federal Government Actions on Cyber Security R&D

Actions	Date	Description
Cyber Security Research and Development Act[a]	November 2002	Enacted to enhance cyber security research efforts. Authorizes the National Science Foundation and the National Institute of Standards and Technology to award grants and establish programs aimed at enhancing computer security and related research partnerships. Defines the responsibility of the Director of the Office of Science and Technology Policy in working with the directors of the National Science Foundation and the National Institute of Standards and Technology to ensure programs authorized by the act are accounted for in governmentwide cyber security research efforts.
National Strategy to Secure Cyberspace	February 2003	Provides direction to the federal government's departments and agencies that have roles in cyberspace security and outlines an initial framework for both organizing and prioritizing efforts. It identifies five national priorities, one of which includes reducing cyberspace threats and vulnerabilities. As part of this priority, the Director of the Office of Science and Technology Policy is to coordinate the development, and update on an annual basis, a federal government R&D agenda for cyber security.
President's Information Technology Advisory Committee report	February 2005	The President's Information Technology Advisory Committee is a federally chartered advisory committee operating under the Federal Advisory Committee Act[b] whose members were appointed by the President to provide independent, expert advice on advanced information technology issues. It conducted a review of the focus, balance, and effectiveness of federally funded cyber security R&D projects. The results of the review were published in a February 2005 report[c] that recommends several changes in the federal government's cyber security R&D portfolio. One of the report's recommendations was to strengthen coordination and oversight of federal cyber security efforts.

Source: GAO analysis of federal policy documents and report.

[a]Pub. L. 107-305, Cyber Security Research and Development Act, November 27, 2002.

[b]Pub. L. 92-463, Federal Advisory Committee Act, October 6, 1972.

[c]President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization* (Washington, D.C.: Feb. 28, 2005).

[5]Pub. L. 94-282, Presidential Science and Technology Advisory Organization Act, May 11, 1976.

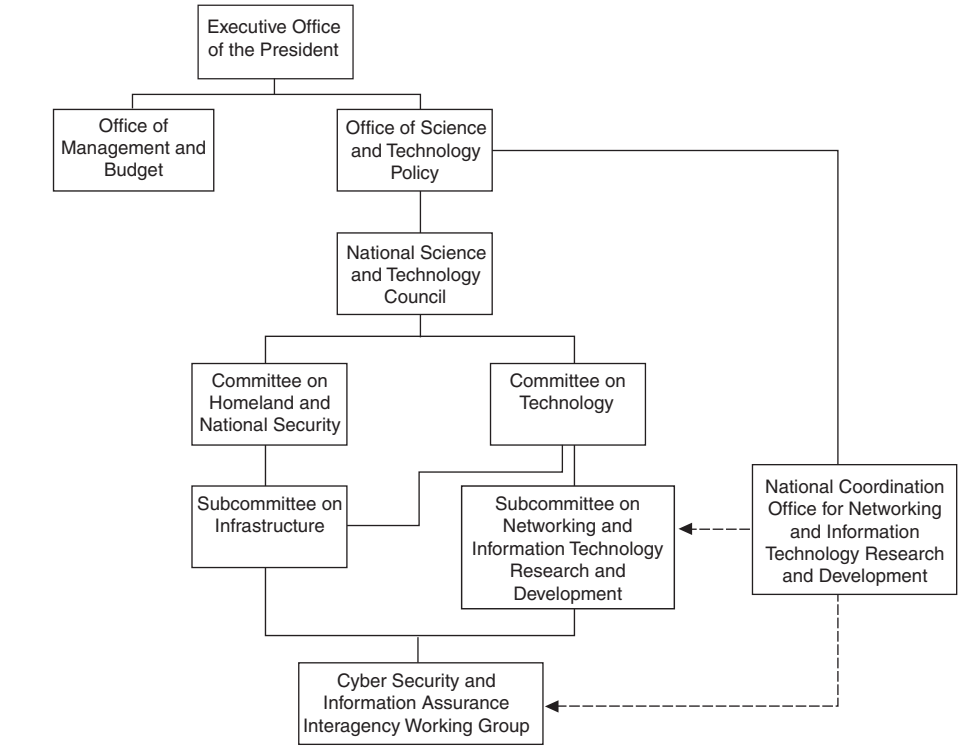
Numerous Federal Entities Involved in Cyber Security Research and Development

Numerous federal agencies and organizations are involved in federally funded cyber security R&D. Several entities oversee and coordinate federal cyber security research; other groups support coordination on an informal basis; and multiple federal agencies fund or conduct this research.

Federal Structure for Oversight and Coordination of Cyber Security Research and Development

The Office of Science and Technology Policy and OMB, both in the Executive Office of the President, provide high-level oversight of federal R&D, including cyber security. The Office of Science and Technology Policy oversees the National Science and Technology Council, which prepares R&D strategies that are 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. The Subcommittee on NITRD and the Interagency Working Group on Cyber Security and Information Assurance are the key entities responsible for coordinating cyber security R&D activities among federal agencies. The organization chart in figure 2 depicts the federal organizations involved.

Figure 2: Organization of Federal Cyber Security R&D Oversight and Coordination



Source: GAO analysis of NITRD information.

While this chart illustrates that several organizations are involved, much of the coordination for cyber security research is actually accomplished at lower level working groups and subcommittees by content matter experts from different agencies. Table 2 contains a brief description of the roles and responsibilities of the federal organizations and groups involved in the oversight and coordination of cyber security research.

Table 2: Federal Organizations Involved in Oversight and Coordination of Cyber Security Research

Organization	Description
Office of Management and Budget	The OMB evaluates, formulates, and coordinates budget and management policies and objectives among federal departments and agencies, including cyber security policies and objectives. Some of its primary responsibilities are to assist the President in developing and maintaining effective government, to develop efficient coordinating mechanisms to expand interagency cooperation, and to develop regulatory reform proposals and programs. In addition, the office has responsibility for developing and maintaining a governmentwide repository of R&D projects.
Office of Science and Technology Policy	The Office of Science and Technology Policy 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. The directors of the Office of Science and Technology Policy and OMB jointly release an annual memorandum to the heads of executive departments and agencies that specifies general R&D budget priorities. Agencies are encouraged to give these priorities full consideration when developing their budget requests, including those related to cyber security. In addition to general program guidance, the memorandums have made interagency R&D efforts (such as the federal NITRD program) a continuing priority.
National Science and Technology Council	The National Science and Technology Council, established in 1993, is the principal means for the administration to coordinate science and technology policy among the diverse parts of the federal areas. The Office of Science and Technology Policy works through the National Science and Technology Council to research and 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.
Committee on Homeland and National Security	The Committee on Homeland and National Security of the National Science and Technology Council increases the productivity and effectiveness of federal science and technology R&D efforts related to homeland and national security. The committee includes representatives from several federal departments, agencies, and organizations within the Executive Office of the President. One of its primary functions is to assist in identifying, defining, and advising the National Science and Technology Council on federal priorities and plans for homeland or national security R&D.
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 being co-chaired by the Department of Commerce and the Office of Science and Technology Policy. Several other agencies or components are members of the committee including the Departments of Homeland Security, Justice, Transportation, and Treasury; and the Central Intelligence Agency.
Subcommittee on Infrastructure	The Subcommittee on Infrastructure is a joint subcommittee that operates under the guidance of the Committee on Homeland and National Security and the Committee on Technology. The subcommittee serves as a forum within the National Science and Technology Council for resolving issues related to the coordination of R&D agendas, policy, and programs associated with the nation's infrastructure. One of the subcommittee's main areas of focus is research related to critical information infrastructure protection.

Organization	Description
Subcommittee on NITRD	Under the guidance of the National Science and Technology Council's Committee on Technology, the Subcommittee on NITRD serves as an internal deliberative organization for networking and information technology R&D policy, program, and budget guidance for the executive branch. Subcommittee members include representatives from 15 federal agencies or components, including the National Science Foundation, Department of Defense, National Security Agency, Defense Advanced Research Projects Agency, and National Institute of Standards and Technology. The Subcommittee on NITRD coordinates the planning, budgeting, and assessment activities of the multi-agency federal NITRD program. This program was chartered under the High-Performance Computing Act of 1991 (Pub.L. 102-194), as amended by the Next Generation Internet Research Act of 1998 (Pub.L. 105-305), to help sustain U.S. leadership in cutting-edge science, engineering, and technology through investments from federal agencies involved in information technology R&D. During fiscal year 2006, agencies participating in NITRD coordinated information technology R&D activities in eight research areas, including cyber security, information assurance, and high-confidence software and systems. Each area has an associated interagency working group or coordinating group of agency program managers that coordinates the planning and activities of its respective research area projects.
National Coordination Office for NITRD	The National Coordination Office for NITRD is responsible for providing technical and administrative support for the Subcommittee on NITRD and interagency activities of the federal NITRD program. This includes helping identify research needs by coordinating interagency meetings as well as conferences and workshops with academia and industry. The National Coordination Office aids information dissemination by publishing reports, including reports produced by the President's Information Technology Advisory Committee, and the annual supplements to the President's budget. To develop the supplements, the National Coordination Office works with OMB to perform a budget analysis of participating NITRD agencies. Technical program and coordination information included in the supplement was gathered during a series of interagency meetings. Although the National Coordination Office assists in the coordination of interagency activities, some coordination responsibilities are conducted at the agency level. For example, while the National Coordination Office collects agency research activities for the development of the budget supplement, it does not provide feedback on program duplication or adherence to strategic priorities. Agencies are expected to weigh other factors during their own prioritization process, including activities of other agencies and perceived research needs from the academic and private-sector research communities. In addition, while agencies participating in classified research provide a valuable threat perspective and additional guidance to interagency meetings, the coordination of classified research is beyond the scope of the NITRD program.

Organization	Description
Interagency Working Group for Cyber Security and Information Assurance	The Cyber Security and Information Assurance Interagency Working Group was chartered in August 2005 to facilitate more coordination of federal cyber security R&D. The working group reports to both the Subcommittee on NITRD and the Subcommittee on Infrastructure. The new charter gives the working group several responsibilities concerning cyber security and information assurance R&D, including 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 the National Science Foundation, the Department of Defense's research organizations, the National Security Agency, the Defense Advanced Research Projects Agency, and the National Institute of Standards and Technology. Other participants include the Central Intelligence Agency and the Departments of Homeland Security, Energy, Justice, State, Transportation, and the Treasury.

Source: GAO analysis of NITRD-provided information.

Other Groups Support Coordination on Informal Basis

Participation by federal entities in other interagency groups provides opportunities for enhanced coordination of cyber security R&D efforts on an informal basis.

InfoSec Research Council

The InfoSec Research Council (the Council) is a voluntary organization that is to facilitate coordination and communication of federal information security research among its members.[6] The Council meets regularly to discuss current research projects, proposed future research initiatives, and critical information security issues. It is also responsible for producing a "hard problems list" that describes what it considers to be the most critical information security problems that, from a government perspective, should be addressed within the next 5 to 10 years. The latest version of the hard problems list was released in November 2005 and includes problems such as addressing insider threats, building secure systems, and improving information security without sacrificing privacy.[7] The development of the list was intended to create consensus on particularly challenging information security issues that can be addressed through federal

[6]The Council's membership includes the Disruptive Technology Office, the Central Intelligence Agency, component agencies of the Department of Defense, the Departments of Energy and Homeland Security, the Federal Aviation Administration, the National Aeronautics and Space Administration, the National Institutes of Health, the National Institute of Standards and Technology, the National Science Foundation, and the Technical Support Working Group.

[7]The November 2005 InfoSec Research Council *Hard Problems List* is publicly available at: http://www.infosec-research.org/documents.html.

government coordination, but the Council recognizes that its members also have their own research priorities.

Technical Support Working Group

The Technical Support Working Group also provides a means for coordination of cyber security R&D. Under the supervision of the Departments of Defense and State, the group operates with the collaboration and voluntary participation of more than 80 federal organizations in its 10 subgroups. In fulfilling its mission to conduct the national interagency R&D program for combating terrorism, the group facilitates interagency communication by serving as a forum for developing user-based counterterrorism technology requirements across the federal government. Its Infrastructure Protection subgroup[8] meets once a year and is responsible for identifying, prioritizing, and executing R&D projects that satisfy interagency infrastructure protection requirements, including cyber security.

Ad Hoc Cooperation

Research and development officials at several agencies noted that, through other informal activities, they maintained additional contact with personnel at other agencies conducting cyber security R&D. Many mentioned that they participated in other agencies' project selection and technical review panels. For example, experts from the Department of Homeland Security served on the review panel for the National Science Foundation's 2005 Cyber Trust program. In addition, officials noted the relatively small size of the federal cyber security research community—many of the same officials attend the coordination meetings and a few officials within the community have worked at other agencies. This familiarity among cyber security experts has allowed for informal knowledge sharing and communication among agencies.

Key Agencies Fund and Conduct Cyber Security Research

While there are multiple agencies involved, three agencies fund and conduct much of cyber security R&D: the National Science Foundation and the Departments of Homeland Security and Defense.

[8]Infrastructure Protection subgroup members include the Environmental Protection Agency, the Nuclear Regulatory Commission, and component agencies of the Departments of Agriculture, Commerce, Defense, Energy, Homeland Security, Justice, and Transportation.

In 2004, the National Science Foundation established the Cyber Trust program to complement ongoing cyber security investments in each of its core research areas: computer and networked systems, computing and communication foundations, information and intelligence systems, shared cyber infrastructure, and information technology research. In accordance with the Cyber Security Research and Development Act, the National Science Foundation awards Cyber Trust grants for projects that (1) advance the relevant knowledge base; (2) creatively integrate research and education for the benefit of technical specialists and the general populace; and (3) effectively integrate the study of technology with the policy, economic, institutional, and usability factors that often determine its deployment and use. Recent Cyber Trust grants include research in areas such as approaches to Internet security, system behavior monitoring, and information security risk management architecture. The President's budget for fiscal year 2006 provides about $94 million to the National Science Foundation for cyber security research, education, and training.

The Department of Homeland Security's R&D efforts are aimed at countering threats to the homeland by making evolutionary improvements to current capabilities and by developing revolutionary new capabilities. The Department of Homeland Security's cyber security R&D program resides in the agency's Science and Technology Directorate. According to Department of Homeland Security officials, the cyber security R&D program was funded—out of the department's $1 billion science and technology budget—with approximately $10 million in fiscal year 2004, $18 million in fiscal year 2005, and $17 million in fiscal year 2006. The Department of Homeland Security's cyber security R&D activities are largely unclassified and near-term.[9] In addition, some work is funded in partnership with the National Science Foundation.

Several agencies within the Department of Defense have cyber security R&D programs. The Department of Defense's Office of the Director, Defense Research and Engineering, provides coordination and oversight in addition to supporting some cyber security research activities directly. The office is responsible for the Department of Defense's science and technology as well as for oversight of research and engineering. According to Department of Defense officials, its cyber security research programs totaled about $150 million in fiscal year 2005. Although the Department of Defense's research organizations (the Office of Naval Research, Army

[9]Near-term is defined as 1–3 years.

Research Laboratory, and Air Force Research Laboratory) have cyber security programs, the largest investments within its cyber security program are with the Defense Advanced Research Projects Agency and the National Security Agency.

The Defense Advanced Research Projects Agency is the central R&D organization of the Department of Defense. Its mission is to identify revolutionary, high-risk, high-payoff technologies of interest to the military—and then to support their development through transition. Its portfolio has shifted toward classified and short-term R&D, and it has the authority to award cash prizes to encourage and accelerate technical accomplishments. There are two types of offices at the agency: technology offices and systems offices. The technology offices focus on new knowledge and component technologies that might have significant national security applications. Systems offices focus on technology development programs leading to products that more closely resemble a specific military end-product; that is, an item that might be in the military's inventory. One of the technology offices (the Information Processing Technology Office) and one of the systems offices (the Advanced Technology Office) focus on cyber security research and development.

The National Security Agency also performs extensive cyber security research. The research is conducted and supported by its National Information Assurance Research Group. Two of the agency's programs—the Information Systems Security Program and Consolidated Cryptologic Program—fund the majority of its cyber security research. The research focuses on high-speed encryption and certain defense capabilities, among other things.

Other Agencies Fund or Conduct Cyber Security Research and Development

In addition to the three primary agencies that fund or conduct cyber security R&D, other agencies, including the Department of Energy, the National Institute of Standards and Technology, and the Disruptive Technology Office, also fund or conduct this research.

The Department of Energy also conducts and funds cyber security R&D. Nearly all of the Department of Energy's cyber security R&D investments are directed toward short-term or military and intelligence applications. This work is conducted principally at the national laboratories.

The National Institute of Standards and Technology's cyber security research program is multi-disciplinary and focuses on a range of long-term to applied R&D in the creation of security standards, guidelines, and new technologies. The National Institute of Standards and Technology's fiscal year 2006 budget estimate for cyber security was $9.1 million. The National Institute of Standards and Technology also receives funding from other agencies such as the Departments of Homeland Security and Transportation and the General Services Administration, to work on projects that are consistent with its cyber security mission. For example, it is producing, for the Department of Homeland Security, the National Vulnerability Database. According to the National Institute of Standards and Technology, it is mandated under the Federal Information Security Management Act, the Cyber Security Research and Development Act, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act (for biometrics), and OMB's Circular A-130, to develop standards, guidelines, and tests for use by federal agencies. Under the Federal Information Security Management Act, the National Institute of Standards and Technology also conducts security research in support of future standards and guidelines.

The Disruptive Technology Office[10] supports the development of technologies to improve the information systems and networks that are used primarily by the intelligence community. Its budget for cyber security research amounts to about $17 million; one third of this amount supports mostly unclassified academic research. However, the office typically classifies the results of this research once it is mature enough to be incorporated into tools for the intelligence community.

Federal Entities Have Improved Oversight and Coordination, but Limitations Remain

Federal entities have taken several important steps to improve the oversight and coordination of federal cyber security R&D. These include (1) chartering an interagency working group to focus on this type of research, (2) publishing a federal plan for cyber security and information assurance research that is to provide baseline information and a framework for planning and conducting this research, (3) separating the reporting of budget information for cyber security research from other

[10]The Disruptive Technology Office, formerly the Advanced Research and Development Activity, moved to the office of the Director of National Intelligence in January 2006. The budget source has also moved.

types of research, and (4) maintaining governmentwide repositories of information on R&D projects. However, limitations exist with the development of a federal cyber security research agenda, the federal plan, and populating the governmentwide repositories that, if not remedied, could diminish the effectiveness of oversight and coordination of cyber security R&D.

Interagency Working Group on Cyber Security Research Provides Coordination Opportunities

In August 2005, the National Science and Technology Council chartered the Interagency Working Group for Cyber Security and Information Assurance. This working group succeeds the Interagency Working Group on Critical Information Infrastructure Protection, which reported to the Subcommittee on Infrastructure. The working group reports jointly to the Subcommittee on NITRD and the Subcommittee on Infrastructure. This change is to facilitate better integration of cyber security R&D with the NITRD program and reflect the broader impact of cyber security and information assurance beyond critical information infrastructure protection. According to a NITRD official, the charter of the Interagency Working Group for Cyber Security and Information Assurance was made in response to the February 2005 recommendation of the President's Information Technology Advisory Committee to strengthen and integrate the working group under the NITRD program.

Federal Plan for Cyber Security Research and Development Has Been Developed but Cyber Security Agenda Still Needed

In February 2003, the National Strategy to Secure Cyberspace was issued to provide a framework for organizing and prioritizing efforts to protect our nation's cyberspace. The strategy recommended that the Director of the Office of Science and Technology Policy coordinate the development of an annual federal government cyber security research agenda that includes near-term (1–3 years), mid-term (3–5 years), and long-term (5 years and longer) research for fiscal years 2004 and beyond.

In April 2006, the Cyber Security and Information Assurance Interagency Working Group released an interagency plan for cyber security research and development.[11] The plan provides baseline information and a technical framework for coordinated multi-agency research in cyber security and information assurance. The Federal Plan for Cyber Security and Information Assurance Research and Development addresses:

[11]Interagency Working Group on Cyber Security and Information Assurance, *Federal Plan for Cyber Security and Information Assurance Research and Development* (Washington, D.C.: April 2006).

- types of vulnerabilities, threats, and risks;
- analysis of recent calls for federal research and development;
- strategic federal objectives;
- technical topics in cyber security and information assurance research;
- current technical and investment priorities of federal agencies in cyber security and information assurance research;
- results of technical and funding gaps analysis;
- findings and recommendations;
- research of technical topic perspectives, including assessments of the state of the art and key technical challenges; and
- a summary of roles and responsibilities, by agency.

According to the Interagency Working Group for Cyber Security and Information Assurance, which operates under the auspices of the Office of Science of Technology Policy and the National Science and Technology Council, the F*ederal Plan for Cyber Security and Information Assurance Research and Development* is the first step towards developing a federal agenda for cyber security research. The plan specifies the need to develop a road map for addressing identified gaps in cyber security research, but has not committed to a date when the road map would be developed or completed.

Key activities for the development of an agenda have not been completed. For instance, mid-term and long-term cyber security research goals have not been defined. Further, the following activities necessary for the agenda have also not been completed: (1) specifying timelines and milestones for conducting research and development activities; (2) specifying goals and measures for evaluating research and development activities; (3) assigning responsibility for implementation, including the accomplishment of the focus areas and suggested research priorities; and (4) aligning the funding priorities with technical priorities.

Until a federal agenda as called for in the *National Strategy to Secure Cyberspace* is developed, increased risk exists that agencies will focus on their individual priorities for cyber security research and development, which may not be the most important national research priorities. Better coordination of research and development efforts will enable the most important topics to receive priority funding and resources and avoid duplication of effort.

Reporting of Budget Information Increases Visibility of Cyber Security Research

For the first time, the NITRD program, in response to the President's Information Technology Advisory Committee recommendation to strengthen coordination,[12] reported budget information for cyber security research separately from other types of research in its supplement to the President's fiscal year 2007 budget. This important change was made possible with the addition of a new NITRD program component area for cyber security and information assurance. Before this addition, budget amounts for cyber security research projects were difficult to identify because they were often grouped with the non-cyber security research projects in other program component areas. Now, program member agencies are to report budget amounts for cyber security research separately. For example, the National Science Foundation, Department of Defense agencies, and National Institute of Standards and Technology, among others, reported budget amounts for cyber security and information assurance research in the NITRD Supplement to the President's Fiscal Year 2007 Budget.

Although the NITRD supplement included budget amounts for cyber security research, this information was limited. Budget amounts for certain cyber security research activities were reported in another NITRD program component area, and budget information on cyber security research for non-NITRD members—such as the Department of Homeland Security and elements within the Department of Energy—was not included in the supplement. However, in his February 2006 testimony before the House Committee on Science, the former Department of Homeland Security Under Secretary for Science and Technology testified that the science and technology division of the Department of Homeland Security is now participating in NITRD. Further, in June 2006, the OMB

[12]The President's Information Technology Advisory Committee listed, as an objective for achieving its recommendation, the systematic collection of data on cyber security R&D efforts throughout the federal government.

issued its annual Circular A-11 budget submission guidance, which requires that agencies submit separate budget amounts for cyber security R&D as part of their 2008 budget submissions. These new requirements should increase the visibility of federal cyber security research and could provide a mechanism for determining the total federal budget in cyber security research and development.

Federal Agencies and Public Could Benefit from Fully Populated Governmentwide Repository

In order to improve the methods by which government information is organized, preserved, and made accessible to the public, the E-Government Act of 2002[13] mandated that the Director of OMB (or the Director's delegate) ensure the development and maintenance of a governmentwide repository and Web site that integrates information about federally funded R&D. The Director delegated this responsibility to the National Science Foundation. According to the E-Government Act, the repository is to integrate information about each separate R&D task or award, including: the dates on which the task or award is expected to start and end, a brief summary describing the objective and the scientific and technical focus of the task or award, the entity performing the task or award, the amount of federal funds to be provided, and any restrictions that would prevent the sharing of information related to the task with the public. In addition, the Web site on which all or part of the repository resides is to be made available to, and be searchable by, federal agencies and non-federal entities, including the general public, and is to facilitate:

- the coordination of federal R&D activities;
- collaboration among those entities conducting federal R&D;
- the transfer of technology among federal agencies, and between federal agencies and non-federal entities; and
- access by policy makers and the public to information concerning federal R&D activities.

The E-Government Act also requires agencies that fund federal R&D to provide the information needed to populate the repository in the manner prescribed by the Director of OMB.

[13]Section 207 (g) Pub. L. 107-347, December 17, 2002.

The federal government has established, and currently funds, two governmentwide repositories and Web sites for R&D information that are available to, and searchable by, federal agencies and the public: Research and Development in the United States (RaDiUS)[14] and Science.gov.[15] RaDiUS is a database that contains information on federally funded R&D projects. Science.gov provides information on federal research through links to science Web sites and scientific databases. The repositories generally contain the type of information about R&D tasks or awards required by the E-Government Act. Both are intended to provide the public and agencies with information about federally funded R&D activities and results.

However, the RaDiUS and Science.gov repositories were incomplete and not fully populated with information about all federally funded tasks and awards. Query searches for cyber security research projects on the RaDiUS repository produced limited results. For example, we found that (1) as of March 2006, all searches on RaDiUS were limited to awards that were made during or prior to fiscal year 2004, (2) searches on RaDiUS for the Department of Homeland Security did not return any cyber-related results and returned only one project when searching for all projects, (3) searches on RaDiUS for the National Science Foundation's Cyber Trust program produced only 8 of the 35 Cyber Trust awards listed for 2004. In addition, the Federal R&D Project Summaries database at Science.gov does not include R&D project summaries for the Departments of Homeland Security and Defense and the National Institute for Standards and Technology. As a result, the usefulness of the repositories and Web sites to facilitate the coordination of cyber security R&D activities, collaboration among researchers, and access to research information in a timely and efficient manner was limited.

[14]Access to RaDiUS is available at https://radius.rand.org.

[15]The Science.gov Federal R&D Project Summaries provides a portal to more than 750,000 Federal research projects, complete with full-text single-query searching across databases residing at different agencies. The portal, a product of the Department of Energy's Office of Scientific and Technical Information, uses research summary and awards data from the Department of Energy, the National Institutes of Health, the National Science Foundation, the Environmental Protection Agency, the Small Business Administration, and the U.S. Department of Agriculture. Access to Science.gov is available at http://www.science.gov.

The governmentwide repositories were incomplete and not fully populated, in part, because OMB had not issued guidance to ensure that agencies had provided all information required for the repositories. Although OMB has issued guidance related to improving the public's access to, and dissemination of, government information and policies for federal agency public Web sites,[16] this guidance does not specifically address reporting information on all federally funded research and development projects to the governmentwide repositories. The E-Government Act specifies that OMB shall issue any guidance determined necessary to ensure that agencies provide all the information required by the act. Our search query results (previously described), and the fact that research and development officials at several federal agencies were not aware of the RaDiUS repository or Web site when asked about the existence of a governmentwide repository for research and development projects indicates that such guidance is necessary.

Federal Agencies Use Various Methods for Technology Transfer

Each of the three primary agencies that fund or conduct cyber security R&D has established technology transfer methods for sharing the results of the research. The following are examples of how each agency conducts technology transfer.

- The National Science Foundation essentially relies on the researcher or grantee to disseminate information about National Science Foundation-funded research. In accordance with the Bayh-Dole Act, the National Science Foundation allows grantees to retain principal legal rights to intellectual property developed under its grants. According to an agency official, the Grant Policy Manual provides the incentive to develop and disseminate inventions, software, and publications that can enhance their usefulness, accessibility, and upkeep. The official stated that the National Science Foundation's policy does not, however, reduce the responsibilities of researchers and organizations to make results, data, and collections available to the research community. It was the National Science Foundation's expectation that grantees would share data, collections, software, and inventions, making their products widely available and useful. The National Science Foundation grantees are required to submit annual and final project reports to the agency; these reports include

[16]The Office of Management and Budget, *Improving Public Access to and Dissemination of Government Information and Using the Federal Enterprise Architecture Data Reference Model* (Washington, D.C.: Dec. 16, 2005) and *Policies for Federal Agency Public Websites* (Washington, D.C.: Dec. 17, 2004).

information on dissemination activities such as publications and conferences.

- The Department of Homeland Security has several methods for technology transfer, such as attending conferences and workshops and working with industry in several areas to share information about emerging threats and R&D needs. In addition, agency officials stated that their Web site is another way that they share information about R&D activities.

- The Department of Defense has several programs to encourage the transfer of technology information. For example, within the academic world, the Department of Defense uses published peer review journals to help facilitate information sharing. Within the classified community, research is shared among the Departments of Defense and Homeland Security and the intelligence community. The Department of Defense's small business innovation research and small business technology transfer programs are used to encourage the transfer of information to the private sector. In addition, every Armed Service research laboratory has a technology transfer office. While technology transfer exists within the Department of Defense, there are instances in which the Department of Defense does not want research information to be available to the public because the information could expose organizational and technological vulnerabilities.

Conclusions

Several federal entities led by the Office of Science and Technology Policy and OMB are involved in overseeing, coordinating, funding, or conducting cyber security R&D. These entities have acted to enhance the oversight and coordination of federal cyber security R&D, including the formation of an interagency working group that developed a federal plan to provide a baseline of information and a technical framework for coordinated multi-agency R&D in cyber security and information assurance. However, key elements of the federal research agenda called for in the National Strategy to Secure Cyberspace have not been developed, thereby increasing the risk that mid- and longer-term research priorities may not be achieved. Without sufficient guidance on reporting R&D information for governmentwide repositories, the repositories cannot be fully populated with data on all cyber security research projects, diminishing their usefulness for coordinating research activities and facilitating technology transfer of research results. Until these issues are addressed, federal research for cyber security and information assurance may not keep pace with the increasing number of threats and vulnerabilities.

Recommendations for Executive Action

To strengthen cyber security research and development programs, we recommend that the Director of the Office of Science and Technology Policy take the following action:

- Establish firm timelines for the completion of the federal cyber security R&D agenda that includes near-term, mid-term, and long-term research. Such an agenda should include the following elements:
- timelines and milestones for conducting research and development activities;
- goals and measures for evaluating research and development activities;
- assignment of responsibility for implementation, including the accomplishment of the focus areas and suggested research priorities; and
- the alignment of funding priorities with technical priorities.

We also recommend that the Director of the Office of Management and Budget implement the following action:

- Issue guidance to agencies on reporting information about federally funded cyber security R&D projects to the governmentwide repositories.

Agency Comments and Our Evaluation

A Senior Policy Analyst in the Office of Science and Technology Policy provided technical comments on a draft of this report, but did not comment on our recommendation that the office establish timelines for the completion of the federal cyber security R&D agenda. We have considered and incorporated the technical comments into the report as appropriate.

In providing oral comments on a draft of this report, OMB officials stated that OMB's August 2006 *Fiscal Year 2006 E-Government Act Reporting Instructions* require agencies that fund federal R&D activities to describe how they fulfill their responsibilities under section 207(g) of the E-Government Act, including how their R&D information is available through RaDiUS, science.gov, or other means. The officials stated that after reviewing the agencies' reports and other information, they will consider whether specific guidance is necessary to further ensure agencies provide all R&D information as required under section 207(g) of the E-Government Act.

In addition, they were concerned with the report's limited scope—cyber security R&D—and stated that the requirement to specify and report cyber security as a separate category of R&D is a recent change and therefore might bias the report's findings. We acknowledge that the scope of our review was limited to cyber security R&D which is why we limited the scope of our findings and recommendations to cyber security R&D. The recent change in reporting requirements relates to the reporting of budgetary information and does not affect our finding on reporting project information to the central repositories.

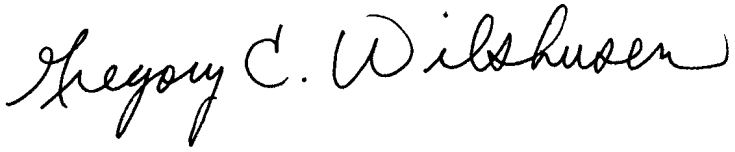
The National Science Foundation and the National Institute of Standards and Technology provided technical comments, which we have incorporated into the report as appropriate.

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

If you or members of your staff have questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or Keith A. Rhodes at (202) 512-6412. We can also be reached by e-mail at wilshuseng@gao.gov and rhodesk@gao.gov, respectively. 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 II.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues

Keith A. Rhodes
Chief Technologist

Appendix I: Objectives, Scope, and Methodology

Our objectives were to identify the (1) federal agencies that are involved with cyber security research and development (R&D); (2) actions taken to improve oversight and coordination of cyber security research and development, including the development of a federal research agenda; and (3) methods used for technology transfer at the agencies with significant activities in cyber security research and development.

To identify which agencies are involved in federal cyber security R&D, we researched a key report on cyber security R&D from the President's Information Technology Advisory Committee. We also analyzed relevant federal law and policy, including the Cyber Security Research and Development Act, the *National Strategy to Secure Cyberspace*, and Homeland Security Presidential Directive 7; we also reviewed our prior reports. We then reviewed budget documents from the Subcommittee on Networking and Information Technology Research and Development (NITRD) to determine the key agencies that fund and conduct cyber security R&D.

To identify actions taken to improve oversight and coordination of federal cyber security R&D, including the development of a governmentwide research agenda, we interviewed officials at the National Science Foundation, the National Institute of Standards and Technology, the National Security Agency, the Departments of Defense and Homeland Security, the Subcommittee on NITRD, the Technical Support Working Group, the Office of Science and Technology Policy, and the Infosec Research Council. We also reviewed NITRD budgetary documents, examined federal policy, reviewed the Office of Management and Budget reports and guidance, observed meetings and reviewed meeting agendas and minutes to determine the extent of coordination for federal cyber security R&D. To evaluate the development of a governmentwide research agenda, we reviewed the *National Strategy to Secure Cyberspace* to determine the requirements for the annual federal cyber security R&D agenda and compared them to the *Federal Plan for Cyber Security and Information Assurance Research and Development* issued by the Interagency Working Group on Cyber Security and Information Assurance. To evaluate the completeness of the RaDiUS repository, in March 2006, we executed search queries on "cybersecurity", "cyber security", "cyber", "cyber trust" and "information assurance" to determine whether the database contained cyber-related program data for the federal agencies. To evaluate the completeness of the Science.gov repositories, in August and September 2006, we executed search queries on "cybersecurity", "cyber security", and "information assurance" to determine whether the database contained cyber-related program data for the federal agencies.

We compared the results to the list of cyber projects provided by the individual agencies. We did not validate the data returned with the agencies conducting cyber security research. In addition, we analyzed relevant laws, including the E-Government Act of 2002 and interviewed officials at the National Science Foundation, the National Institute of Standards and Technology, the National Security Agency, and the Departments of Defense and Homeland Security to evaluate the completeness of the two mandated governmentwide repositories.

To identify methods used for technology transfer at the agencies with significant cyber security research activities, we identified the agencies and other groups that have responsibility for management and oversight of federal cyber security R&D, interviewed officials at these agencies to determine their methods for technology transfer, and reviewed agency policies on technology transfer. We also analyzed relevant laws, including the Bayh-Dole Act.

We conducted our work from August 2005 through August 2006 in accordance with generally accepted government auditing standards.

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Keith A. Rhodes, (202) 512-6412 or rhodesk@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Kristi Dorsey, Nalani Fraser, Nancy Glover, Richard Hung, Anjalique Lawrence, and Suzanne Lightman were key contributors to this report.

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, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548