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.