June 2010

CYBERSECURITY

Key Challenges Need to Be Addressed to Improve Research and Development

GAO Accountability • Integrity • Reliability

Highlights

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

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.