March 10, 2009

NATIONAL CYBERSECURITY STRATEGY

Key Improvements Are Needed to Strengthen the Nation's Posture

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-432T, a testimony to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Pervasive and sustained computer-based (cyber) attacks against federal and private-sector infrastructures pose a potentially devastating impact to systems and operations and the critical infrastructures that they support. To address these threats, President Bush issued a 2003 national strategy and related policy directives aimed at improving cybersecurity nationwide. Congress and the Executive Branch, including the new administration, have subsequently taken actions to examine the adequacy of the strategy and identify areas for improvement. Nevertheless, GAO has identified this area as high risk and has reported on needed improvements in implementing the national cybersecurity strategy.

In this testimony, you asked GAO to summarize (1) key reports and recommendations on the national cybersecurity strategy and (2) the views of experts on how to strengthen the strategy. In doing so, GAO relied on its previous reports related to the strategy and conducted panel discussions with key cybersecurity experts to solicit their views on areas for improvement.

What GAO Recommends

GAO has previously made about 30 recommendations, mostly directed at DHS, to improve our nation's cybersecurity strategy efforts. DHS in large part has concurred with GAO's recommendations and, in many cases, has actions planned and under way to implement them.

View GAO-09-432T or key components. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Over the last several years, GAO has consistently reported that the Department of Homeland Security (DHS) has yet to fully satisfy its responsibilities designated by the national cybersecurity strategy. To address these shortfalls, GAO has made about 30 recommendations in key cybersecurity areas including the 5 listed in the table below. While DHS has since developed and implemented certain capabilities to satisfy aspects of its cybersecurity responsibilities, it still has not fully satisfied the recommendations, and thus further action needs to be taken to fully address these areas.

Key Cybersecurity Areas Identified by GAO as Needing Further Action
1. Bolstering cyber analysis and warning capabilities
2. Completing actions identified during cyber exercises
3. Improving cybersecurity of infrastructure control systems
4. Strengthening DHS's ability to help recover from Internet disruptions
5. Addressing cybercrime

Source: GAO analysis of prior GAO reports.

In discussing the areas addressed by GAO's recommendations as well as other critical aspects of the strategy, GAO's panel of cybersecurity experts identified 12 key areas requiring improvement (see table below). GAO found these to be largely consistent with its reports and its extensive research and experience in the area.

Key Strategy Improvements Identified by Cybersecurity Experts	
1.	Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.
2.	Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
3.	Establish a governance structure for strategy implementation.
4.	Publicize and raise awareness about the seriousness of the cybersecurity problem.
5.	Create an accountable, operational cybersecurity organization.
6.	Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7.	Bolster public/private partnerships through an improved value proposition and use of incentives.
8.	Focus greater attention on addressing the global aspects of cyberspace.
9.	Improve law enforcement efforts to address malicious activities in cyberspace.
10.	Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts.
11.	Increase the cadre of cybersecurity professionals.
12.	Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

Until GAO's recommendations are fully addressed and the above improvements are considered, our nation's federal and private-sector infrastructure systems remain at risk of not being adequately protected. Consequently, in addition to fully implementing GAO's recommendations, it is essential that the improvements be considered by the new administration as it begins to make decisions on our nation's cybersecurity strategy.