G A O
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-10-606, a report to congressional requesters

July 2010

CYBERSPACE

United States Faces Challenges in Addressing Global Cybersecurity and Governance

Why GAO Did This Study

Recent foreign-based intrusions on the computer systems of U.S. federal agencies and commercial companies highlight the vulnerabilities of the interconnected networks that comprise the Internet, as well as the need to adequately address the global security and governance of cyberspace. Federal law and policy give a number of federal entities responsibilities for representing U.S. cyberspace interests abroad, in collaboration with the private sector. More recently, the President appointed a national Cybersecurity Coordinator charged with improving the nation's cybersecurity leadership. GAO was asked to identify (1) significant entities and efforts addressing global cyberspace security and governance issues, (2) U.S. entities responsible for addressing these issues and the extent of their involvement at the international level, and (3) challenges to effective U.S. involvement in global cyberspace security and governance efforts. To do this, GAO analyzed policies, reports, and other documents and interviewed U.S. government and international officials and experts from over 30 organizations.

What GAO Recommends

GAO recommends that the national Cybersecurity Coordinator address challenges including developing a comprehensive national global cyberspace strategy. The national Cybersecurity Coordinator and his staff generally concurred with the recommendations and stated that actions are already being taken.

View GAO-10-606 or key components.
For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

There are a number of key entities and efforts with significant influence on international cyberspace security and governance. The organizations range from information-sharing forums that are nondecision-making gatherings of experts to private organizations to treaty-based, decision-making bodies founded by countries. Their efforts include those to address topics such as incident response, technical standards, and law enforcement cooperation. For example, the International Organization for Standardization is a nongovernmental organization that develops and publishes international standards, including those related to cybersecurity, through a consensus-based process involving a network of the national standards bodies of 162 countries.

A number of U.S. federal entities have responsibilities for, and are involved in, international cyberspace governance and security efforts. Specifically, the Departments of Commerce, Defense, Homeland Security, Justice, and State, among others, are involved in efforts to develop international standards, formulate cyber-defense policy, facilitate overseas investigations and law enforcement, and represent U.S. interests in international forums. Federal entities have varying roles among organizations and efforts with international influence over cyberspace security and governance, including engaging in bilateral and multilateral relationships with foreign countries, providing personnel to foreign agencies, leading or being a member of a U.S. delegation, coordinating U.S. policy with other U.S. entities through the interagency process, or attending meetings.

The global aspects of cyberspace present key challenges to U.S. policy (see table). Until these challenges are addressed, the United States will be at a disadvantage in promoting its national interests in the realm of cyberspace.

U.S. Challenges in Addressing Global Cybersecurity and Governance

Challenge	Description
Leadership	Providing top-level leadership that can coordinate across federal entities and forge a coherent national approach.
Strategy	Developing a comprehensive national strategy that specifies overarching goals, subordinate objectives, activities to support those objectives, and outcome-oriented performance metrics and time frames.
Coordination	Engaging all key federal entities in order to coordinate policy related to global aspects of cyberspace security and governance.
Standards and policies	Ensuring that international technical standards and polices do not pose unnecessary barriers to U.S. trade.
Incident response	Participating in international cyber-incident response, which includes appropriately sharing information without jeopardizing national security.
Differing law	Investigating and prosecuting transnational cybercrime amid a plurality of laws, varying technical capabilities, and differing priorities.
Norms	Providing models of behavior that shape the policies and activities of countries, such as defining countries' sovereign responsibility regarding the actions of its citizens.

Source: GAO analysis of federal and nonfederal information.