May 2004

TECHNOLOGY ASSESSMENT

Cybersecurity for Critical Infrastructure Protection

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-321, a report to congressional requesters

Why GAO Did This Study

Computers are crucial to the operations of government and business. Computers and networks essentially run the critical infrastructures that are vital to our national defense, economic security, and public health and safety. Unfortunately, many computer systems and networks were not designed with security in mind. As a result, the core of our critical infrastructure is riddled with vulnerabilities that could enable an attacker to disrupt operations or cause damage to these infrastructures. Critical infrastructure protection (CIP) involves activities that enhance the security of our nation's cyber and physical infrastructure. Defending against attacks on our information technology infrastructure—cybersecurity—is a major concern of both the government and the private sector. Consistent with guidance provided by the Senate's Fiscal Year 2003 Legislative Branch Appropriations Report (S. Rpt. 107-209), GAO conducted this technology assessment on the use of cybersecurity technologies for CIP in response to a request from congressional committees. This assessment addresses the following questions: (1) What are the key cybersecurity requirements in each of the CIP sectors? (2) What cybersecurity technologies can be applied to CIP? (3) What are the implementation issues associated with using cybersecurity technologies for CIP, including policy issues such as privacy and information sharing?

www.gao.gov/cgi-bin/getrpt?GAO-04-321.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Keith Rhodes at (202) 512-6412 or rhodesk@gao.gov.

What GAO Found

Many cybersecurity technologies that can be used to protect critical infrastructures from cyber attack are currently available, while other technologies are still being researched and developed. These technologies, including access control technologies, system integrity technologies, cryptography, audit and monitoring tools, and configuration management and assurance technologies, can help to protect information that is being processed, stored, and transmitted in the networked computer systems that are prevalent in critical infrastructures.

Although many cybersecurity technologies are available, experts feel that these technologies are not being purchased or implemented to the fullest extent. An overall cybersecurity framework can assist in the selection of technologies for CIP. Such a framework can include (1) determining the business requirements for security; (2) performing risk assessments; (3) establishing a security policy; (4) implementing a cybersecurity solution that includes people, processes, and technologies to mitigate identified security risks; and (5) continuously monitoring and managing security. Even with such a framework, other demands often compete with cybersecurity. For instance, investing in cybersecurity technologies often needs to make business sense. It is also important to understand the limitations of some cybersecurity technologies. Cybersecurity technologies do not work in isolation; they must work within an overall security process and be used by trained personnel. Despite the availability of current cybersecurity technologies, there is a demonstrated need for new technologies. Long-term efforts are needed, such as the development of standards, research into cybersecurity vulnerabilities and technological solutions, and the transition of research results into commercially available products.

There are three broad categories of actions that the federal government can undertake to increase the use of cybersecurity technologies. First, it can take steps to help critical infrastructures determine their cybersecurity needs, such as developing a national CIP plan, assisting with risk assessments, and enhancing cybersecurity awareness. Second, the federal government can take actions to protect its own systems, which could lead others to emulate it or could lead to the development and availability of more cybersecurity technology products. Third, it can undertake long-term activities to increase the quality and availability of cybersecurity technologies in the marketplace.

Ultimately, the responsibility for protecting critical infrastructures falls on the critical infrastructure owners. However, the federal government has several options at its disposal to manage and encourage the increased use of cybersecurity technologies, research and develop new cybersecurity technologies, and generally improve the cybersecurity posture of critical infrastructure sectors.