January 2003

CRITICAL INFRASTRUCTURE PROTECTION

Efforts of the Financial Services Sector to Address Cyber Threats

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-173, a report to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Growth, Committee on Financial Services, House of Representatives

Why GAO Did This Study

Since 1998, the federal government has taken steps to protect the nation's critical infrastructures, including developing partnerships between the public and private sectors. These cyber and physical public and private infrastructures, which include the financial services sector, are essential to national security, economic security, and/or public health and safety.

GAO was asked to review (1) the general nature of the cyber threats faced by the financial services industry; (2) steps the financial services industry has taken to share information on and to address threats, vulnerabilities, and incidents; (3) the relationship between government and private sector efforts to protect the financial services industry's critical infrastructures; and (4) actions financial regulators have taken to address these cyber threats.

What GAO Recommends

GAO recommends that Treasury (1) coordinate with the industry in its efforts to update the sector's strategy and establish detailed plans for implementing it and (2) assess the need for public policy tools to assist the industry. In comments on a draft of this report, Treasury recognized the need to continue to work with the sector to increase its resiliency, including consideration of appropriate incentives. Other agencies and private sector entities provided technical comments, which were addressed as appropriate.

www.gao.gov/cgi-bin/getrpt?GAO-03-173.

To view the full report, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or Daceyr@gao.gov.

What GAO Found

The types of cyber threats that the financial services industry faces are similar to those faced by other critical infrastructure sectors: attacks from individuals and groups with malicious intent, such as crime, terrorism, and foreign intelligence. However, the potential for monetary gains and economic disruptions may increase its attractiveness as a target.

Financial services industry groups have taken steps and plan to take continuing action to address cyber threats and improve information sharing. First, industry representatives, under the sponsorship of the U.S. Department of the Treasury, collaboratively developed a sector strategy which discusses additional efforts necessary to identify, assess, and respond to sectorwide threats. However, the financial services sector has not developed detailed plans for implementing its strategy. Second, the private sector's Financial Services Information Sharing and Analysis Center was formed to facilitate sharing of cyber-related information. Third, several other industry groups are taking steps to better coordinate industry efforts and to improve information security across the sector.

Several federal entities play critical roles in partnering with the private sector to protect the financial services industry's critical infrastructures. For example, the Department of the Treasury is the sector liaison for coordinating public and private efforts and chairs the federal Financial and Banking Information Infrastructure Committee, which coordinates regulatory efforts. As part of its efforts, Treasury has taken steps designed to establish better relationships and methods of communication between regulators, assess vulnerabilities, and improve communications within the financial services sector. In its role as sector liaison, Treasury has not undertaken a comprehensive assessment of the potential use of public policy tools by the federal government to encourage increased participation by the private sector. The table below shows the key public and private organizations involved in critical infrastructure protection.

Key Critical Infrastructure Protection Organizations in the Financial Services Industry

Public Sector	Private Sector
• Sector Liaison/Assistant Secretary for Financial Institutions - Department of the Treasury • Special Advisor to the President for Cyberspace Security • Financial and Banking Information Infrastructure Committee • National Infrastructure Protection Center • Critical Infrastructure Assurance Office	• Sector Coordinator • Financial Services Sector Coordinating Council • Financial Services Information Sharing and Analysis Center • Trade Associations (e.g. American Bankers Association, BITS, Securities Industry Association)

Source: GAO analysis.

Federal regulators, such as the Federal Reserve System and the Securities and Exchange Commission, have taken steps to address information security issues. These include consideration of information security risks in determining the scope of their examinations of financial institutions and development of guidance for examining information security and for protecting against cyber threats.