United States General Accounting Office

GAO

Report to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Growth, Committee on Financial Services, House of Representatives

January 2003

CRITICAL INFRASTRUCTURE PROTECTION

Efforts of the Financial Services Sector to Address Cyber Threats

GAO-03-173

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.

Contents

Abbreviations

ABA	American Bankers Association
CIAO	Critical Infrastructure Assurance Office
CIP	critical infrastructure protection
FBI	Federal Bureau of Investigation
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examinations Council
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council
ISACs	Information Sharing and Analysis Centers
NCUA	National Credit Union Administration
NIPC	National Infrastructure Protection Center
OCC	Office of the Comptroller of the Currency
OTS	Office of Thrift Supervision
PDD 63	Presidential Decision Directive 63
SEC	Securities and Exchange Commission
SIA	Securities Industry Association
URSIT	Uniform Rating System for Information Technology

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

January 30, 2003

The Honorable Peter T. King
Chairman
The Honorable Carolyn B. Maloney
Ranking Minority Member
Subcommittee on Domestic Monetary Policy, Technology,
and Economic Growth
Committee on Financial Services
House of Representatives

The federal government has identified the financial services sector as part of its critical infrastructure protection (CIP) efforts. Critical infrastructures are those cyber and physical public and private infrastructures that are essential to national security, economic security, and/or public health and safety. The U.S. financial services sector—which includes commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, thrift institutions, securities brokers and dealers, and others[1]—held over $23.5 trillion in assets as of the second quarter of 2002.[2]

The use of computer interconnectivity by the financial services sector[3] for customer services, such as Internet banking and electronic securities trading, and for business operations, such as clearing and settlement,[4] has increased the degree of access to the systems used to support these services. This increased access poses significant information security risks

[1]*Defending America's Cyberspace: Banking and Finance Sector: The National Strategy for Critical Infrastructure Assurance, Version 1.0*, May 13, 2002.

[2]Board of Governors of the Federal Reserve System, *Federal Reserve statistical release, Flow of Funds Accounts of the United States: Flows and Outstandings Second Quarter 2002* (Washington, D.C.: Sept. 16, 2002).

[3]Some industry groups, such as the Financial Services Information Sharing and Analysis Center, use the term "financial services" to describe the sector they represent. Documents related to critical infrastructure protection, including Presidential Decision Directive 63, issued in May 1998, and the *National Strategy for Homeland Security*, issued in July 2002, refer to the sector as the banking and finance sector. In this report we use the terms "financial services sector," "financial services industry," and the "banking and finance sector" interchangeably.

[4]Clearing and settlement is the processing of transactions, e.g., securities trades and checks.

to computer systems and to the critical operations and infrastructures they support, if those systems are not properly secured.

In response to your request, we identified (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. To accomplish these objectives, we reviewed relevant documents, policy, and directives and interviewed pertinent officials from federal agencies and the private sector involved in efforts to enhance the security of the financial services industry. Appendix I provides further details on our objectives, scope, and methodology.

Results in Brief

The types of cyber threats that the financial services sector 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. At the same time, sector representatives believe that financial institutions recognize and work to mitigate the threat in order to adhere to federal and state regulations and maintain public confidence in their ability to protect and manage customer assets. However, financial services institutions have experienced cyber incidents that have had some impact on their operations, which demonstrates a continuing threat to the industry. In addition, the financial services sector faces vulnerability because of its dependence on other critical infrastructures. For example, threats facing the telecommunications and power sectors could directly affect the financial services industry.

Financial services industry groups have taken several steps to address cyber threats and improve information sharing and plan to take continuing action to further address these issues. First, industry representatives worked collaboratively on a Treasury-sponsored working group to develop the sector's *National Strategy for Critical Infrastructure Assurance*, which was issued in May 2002. The strategy discusses additional efforts necessary to identify, assess, and respond to sectorwide threats, including completing a sectorwide vulnerability assessment. However, the financial services sector has not developed detailed interim objectives; detailed tasks, timeframes, or responsibilities for implementation; or processes for

measuring progress in implementing the sector's strategy. Second, the private sector's Financial Services Information Sharing and Analysis Center was formed in October 1999 to, among other objectives, facilitate sharing of information and provide its members with early notification of computer vulnerabilities and attacks. Third, major sector associations, professional institutes, national exchanges, and other broad industry organizations recently formed the Financial Services Sector Coordinating Council for Critical Infrastructure Protection/Homeland Security to better foster and facilitate coordination of sectorwide efforts. In addition, several other financial services industry groups, such as the American Bankers Association, the Financial Services Roundtable/BITS, the Securities Industry Association, and other trade groups, are taking steps to improve information security and business continuity practices across their memberships and the sector.

Several federal entities play critical roles in partnering with the financial services sector to protect critical infrastructures. Treasury is the lead federal agency, or sector liaison, responsible for coordinating with the financial services sector and, in particular, the sector coordinator—the private-sector focal point for the industry. Treasury also chairs the Financial and Banking Information Infrastructure Committee of the President's Critical Infrastructure Protection Board. The committee is responsible for coordinating federal and state financial regulatory efforts to improve the reliability and security of U.S. financial systems. 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. However, in its role as sector liaison, Treasury has not undertaken a comprehensive assessment, as called for in federal CIP policy, of the potential use of public policy tools, such as grants, tax incentives, and regulation, to encourage the financial services sector in implementing CIP-related efforts. In addition to Treasury's efforts, other federal CIP-related entities have taken steps to encourage the participation of the financial services sector in CIP.

Federal regulators, such as the Federal Reserve System and the Securities and Exchange Commission, have taken several 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.

To improve the likelihood of success of the sector's CIP efforts, we are recommending that the Secretary of the Treasury direct the Assistant Secretary for Financial Institutions, the financial services sector liaison, to coordinate with the industry in its efforts to update the sector's *National Strategy for Critical Infrastructure Assurance* and in establishing interim objectives; detailed tasks, timeframes, and responsibilities for implementing it; and a process for monitoring progress. As part of these efforts, Treasury should assess the need for grants, tax incentives, regulation, or other public policy tools to assist the industry in meeting the sector's goals.

We received written comments on a draft of this report from the Department of the Treasury and the Securities and Exchange Commission (see apps. II and III, respectively). The Department of the Treasury highlighted its efforts and recognized the need to continue to work with the sector to increase its resiliency, including consideration of appropriate incentives. The Securities and Exchange Commission stated that it looked forward to working with Treasury to implement the recommendations. We received technical comments from the Federal Deposit Insurance Corporation, the FBI's National Infrastructure Protection Center, the Federal Reserve, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission. In addition, we received written and oral technical comments from private-sector participants. Comments from all of these organizations have been incorporated into the report, as appropriate. The Department of Commerce's Critical Infrastructure Assurance Office, the Office of Thrift Supervision, and the National Credit Union Association reviewed a draft of the report and had no comments.

Background

CIP Policy Has Been Evolving since the Mid-1990's; Financial Services Sector Has Always Been Considered Critical

Federal awareness of the importance of securing our nation's critical infrastructures, which underpin our society, economy, and national security, has been evolving since the mid-1990's. Over the years, a variety of working groups has been formed, special reports have been written, federal policies issued, and organizations created to address the issues that have been raised.

In October 1997, the President's Commission on Critical Infrastructure Protection issued its report,[5] describing the potentially devastating implications of poor information security from a national perspective. The report recommended several measures to achieve a higher level of CIP, including infrastructure protection through industry cooperation and information sharing, a national organization structure, a revised program of research and development, a broad program of awareness and education, and reconsideration of laws related to infrastructure protection. The report stated that a comprehensive effort would need to "include a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyberthreats." The financial services sector was highlighted as one of several critical infrastructures that were vital to our nation's economic security.

In 1998, the President issued Presidential Decision Directive 63 (PDD 63), which established CIP as a national goal and described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. PDD 63 called for a range of actions intended to improve federal agencies' security programs, improve the nation's ability to detect and respond to serious computer-based and physical attacks, and establish a partnership between the government and the private sector. The directive called on the federal government to serve as a model of how infrastructure assurance is best achieved and designated lead agencies to work with private-sector and government organizations.

To accomplish its goals, PDD 63 established and designated organizations to provide central coordination and support, including

- the Critical Infrastructure Assurance Office (CIAO), an interagency office housed in the Department of Commerce, which was established to develop a national plan for CIP on the basis of infrastructure plans developed by the private sector and federal agencies;

- the National Infrastructure Protection Center (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response; and

[5] *Critical Foundations: Protecting America's Infrastructures*, Report of the President's Commission on Critical Infrastructure Protection (October 1997).

- the National Infrastructure Assurance Council, which was established to enhance the partnership of the public and private sectors in protecting our critical infrastructures.[6]

To ensure coverage of critical sectors, PDD 63 also identified eight private-sector infrastructures, including banking and finance, and five special functions.[7] For each of the infrastuctures and functions, the directive designated lead federal agencies, known as sector liaisons, to work with their counterparts in the private sector, known as sector coordinators. For example, Treasury is responsible for working with the financial services sector, and the Department of Energy is responsible for working with the electrical power industry. Similarly, regarding special function areas, the Department of Defense is responsible for national defense, and the Department of State is responsible for foreign affairs.

PDD 63 called for a range of actitivites intended to establish a partnership between the public and private sectors to ensure the security of our nation's critical infrastructures. The sector liaison and the sector coordinator were to work with each other to address problems related to CIP for their sector. In particular, PDD 63 stated that they were to (1) develop and implement a vulnerability awareness and education program and (2) contribute to a sectoral National Infrastructure Assurance Plan by

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing major attacks; and

[6]Executive Order 13231 (October 2001) replaces this council with the National Infrastructure Advisory Council.

[7]The infrastructures were (1) banking and finance; (2) information and communications; (3) water supply; (4) aviation, highway, mass transit, pipelines, rail, and waterborne commerce; (5) emergency law enforcement; (6) emergency fire services and continuity of government; (7) electric power and oil and gas production and storage; and (8) public health services. The special functions were (1) law enforcement and internal security, (2) intelligence, (3) foreign affairs, (4) national defense, and (5) research and development.

- developing a plan for alerting, containing, and rebuffing an attack in progress and then, in coordination with the Federal Emergency Management Agency as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

PDD 63 also stated that sector liaisons should identify and assess economic incentives to encourage the desired sector behavior in CIP. Further, to facilitate private-sector participation, it encouraged the voluntary creation of information sharing and analysis centers (ISACs) that could serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC.

In response to PDD 63, a banking and finance sector coordinating committee on CIP, chaired by a sector coordinator, was initiated by the Secretary of the Treasury in October 1998.[8] In addition, the Financial Services ISAC (FS-ISAC) was formed in 1999.

In January 2000, the White House issued its *National Plan for Information Systems Protection*.[9] The national plan provided a vision and a framework for the federal government to prevent, detect, respond to, and protect the nation's critical cyber-based infrastructure from attack and reduce existing vulnerabilities by complementing and focusing existing federal computer security and information technology requirements. Subsequent versions of the plan were expected to (1) define the roles of industry and of state and local governments working in partnership with the federal government to protect physical and cyber-based infrastructures from deliberate attack and (2) examine the international aspects of CIP.

In October 2001, the President signed Executive Order 13231, establishing the President's Critical Infrastructure Protection Board to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures. The Special Advisor to the President for Cyberspace Security chairs the board. Executive Order 13231 tasks the

[8]In June 2002, the Financial Services Sector Coordinating Council (FSSCC), organized and chaired by the current sector coordinator, replaced the banking and finance sector coordinating committee on CIP. According to the current sector coordinator, the former committee was a more ad hoc effort and did not include the entire financial services sector.

[9]The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* (Washington, D.C.: 2000).

board with recommending policies and coordinating programs for protecting CIP-related information systems. The board was intended to coordinate with the Office of Homeland Security in activities related to protection and recovery from attacks against information systems for critical infrastructure, including emergency preparedness communications that were assigned to the Office of Homeland Security by Executive Order 13228, dated October 8, 2001. According to Executive Order 13231, the board recommends policies and coordinates programs for protecting information systems for critical infrastructures, including emergency preparedness communications and the physical assets that support such systems. The Special Advisor reports to the Assistant to the President for National Security Affairs and to the Assistant to the President for Homeland Security. In addition, the Special Advisor, as chair of the board, coordinates with the Assistant to the President for Economic Policy on issues related to private-sector systems and economic effects and with the Director of the Office of Management and Budget (OMB) on issues related to budgets and the security of federal computer systems. Executive Order 13231 reiterated the importance and voluntary nature of the Information Sharing and Analysis Centers (ISACs).

Executive Order 13231 also established 10 standing committees to support the board's work on a wide range of critical infrastructure efforts. The Financial and Banking Information Infrastructure Committee (FBIIC), one of the standing committees, is charged with coordinating federal and state financial regulatory efforts to improve the reliability and security of the U.S. financial system. Chaired by the Department of the Treasury's Assistant Secretary for Financial Institutions, FBIIC includes representatives from federal and state financial regulatory agencies, including the Commodity Futures Trading Commission, the Conference of State Bank Supervisors, the Federal Deposit Insurance Corporation (FDIC), the Federal Housing Finance Board, the Federal Reserve Bank of New York, the Federal Reserve Board, the National Association of Insurance Commissioners (NAIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), the Office of Federal Housing Enterprise Oversight, the Office of Homeland Security, the Office of Cyberspace Security, the Office of Thrift Supervision (OTS), and the Securities and Exchange Commission (SEC).

Consistent with PDD 63, industry representatives worked collaboratively on a Treasury-sponsored working group to develop the sector's national strategy—*Defending America's Cyberspace: Banking and Finance Sector: The National Strategy for Critical Infrastructure Assurance, Version 1.0.*

Treasury's Assistant Secretary for Financial Institutions submitted the industry's strategy, in May 2002, to the Special Advisor to the President for Cyberspace Security, with the understanding that it would provide an evolving baseline for the sector's efforts.

In July 2002, the President issued the *National Strategy for Homeland Security* to "mobilize and organize our nation to secure the United States homeland from terrorist attacks." According to the strategy, the primary objectives of homeland security, in order of priority, are to (1) prevent terrorist attacks within the United States, (2) reduce America's vulnerability to terrorism, and (3) minimize the damage and recover from attacks that do occur. The strategy identifies two critical components of CIP—critical infrastructure and intelligence and warning—as two of six mission areas.[10] The strategy further states that if terrorists attack one or more pieces of our critical infrastructure, they may disrupt entire systems and significantly damage the nation. In addition, the national strategy continues to identify banking and finance as a critical infrastructure sector, and it adds additional sectors, as shown in table 1.

[10]The other four mission areas are border and transportation security, domestic terrorism, defending against catastrophic terrorism, and emergency preparedness and response.

Table 1: Critical Infrastructure Lead Agencies

Lead agency	Sectors
Homeland Security	information and telecommunications transportation (aviation, rail, mass transit, waterborne commerce, pipelines, and highways, including trucking and intelligent transportation systems) postal and shipping emergency services continuity of government
Treasury	banking and finance
Health and Human Services	public health (including prevention, surveillance, laboratory services, and personal health services) food (all except for meat and poultry)
Energy	energy (electrical power, oil and gas production, and storage)
Environmental Protection Agency	water chemical industry and hazardous materials
Agriculture	agriculture food (meat and poultry)
Defense	defense industrial base

Source: National Strategy for Homeland Security and PDD 63.

On September 18, 2002, the administration released a draft *National Strategy to Secure Cyberspace*.[11] The draft was developed by the President's Critical Infrastructure Protection Board on the basis of input from officials associated with key sectors of the economy that rely on cyberspace, state and local governments, colleges and universities, and others. The draft strategy contains 86 recommendations for home users and small businesses; large private-sector corporations; federal, state, and local governments; critical sectors; and colleges and universities—among others. The draft strategy supplements existing strategies, including the *National Strategy for Homeland Security*, and states that the strategies' policy statements and recommendations are subject to Executive Order 13231 and other relevant executive orders related to national security. The draft strategy calls for the continued use of public/private partnerships established through the lead federal agencies and the private-sector coordinators and the ISACs. The draft strategy is consistent with the *National Strategy for Homeland Security* concerning lead agency responsibilities.

[11]The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace for Comment (Draft)* (Washington, D.C.: Sept. 18, 2002).

On November 25, 2002, the President signed the Homeland Security Act of 2002, establishing the Department of Homeland Security. Regarding critical infrastructure protection, the new department is responsible for, among other things, (1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States; (2) recommending measures to protect the key resources and critical infrastructure of the United States in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities; and (3) disseminating, as appropriate, information analyzed by the department—both within the department and to other federal agencies, state and local government agencies, and private sector entities—to assist in the deterrence, prevention, preemption of, or response to terrorist attacks. The act also transfers the functions, personnel, assets, and liabilities of NIPC (other than the Computer Investigations and Operations Section) and CIAO to the new department.

Overview of the Financial Industry and Financial Regulators

According to statistics from the Federal Reserve Board,[12] U.S. financial institutions held over $23.5 trillion in assets as of the second quarter of 2002—about a $2 trillion dollar increase over first quarter 2001 statistics reported in the sector's national strategy. Some of the largest categories of financial institutions are commercial banks ($5.3 trillion), insurance companies ($2.7 trillion), mutual funds ($2.7 trillion), government-sponsored enterprises ($2.2 trillion), and pension funds ($1.5 trillion). The remaining assets are distributed among finance and mortgage companies, securities brokers and dealers, and other financial institutions.

The sector's national strategy states that the composition of the financial services sector extends beyond these companies to include a network of essential specialized service organizations and service providers who support the sector in its efforts to provide a trusted services environment; these include securities and commodities exchanges, funds transfer networks, payment networks, clearing companies, trust and custody firms, and depositories and messaging systems. According to the national strategy, the financial services sector has also become more dependent on outsourcing certain activities—such as systems and applications, hardware

[12]Board of Governors of the Federal Reserve System, *Federal Reserve statistical release, Flow of Funds Accounts of the United States: Flows and Outstandings Second Quarter 2002* (Washington, D.C.: Sept. 16, 2002).

and software, as well as technically skilled personnel—to third-party providers that are an indispensable part of the sector's infrastructure.

Several regulatory agencies oversee various aspects of the financial services industry. Table 2 provides an overview of the key industry segments and the regulatory bodies that oversee them. Five federal regulators—the Federal Reserve System (FRS), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), and the National Credit Union Administration (NCUA)—supervise and examine all federally insured depository institutions. The regulators oversee a mix of large, medium, and small depository institutions, as shown in table 3. Banking regulators also work together through the Federal Financial Institutions Examinations Council (FFIEC),[13] an interagency forum that Congress created in 1979 to promote consistency in the examination and supervision of depository institutions. For example, the Information Technology Subcommittee of the FFIEC Task Force on Supervision supervises the largest 18 to 20 technology service providers, and the regulators' regional offices supervise smaller technology service providers. The regulators also issue policies, procedures, rules, legal interpretations, and corporate decisions concerning banking, credit, bank investments, asset management, fair lending and consumer protection, community reinvestment activities, and other aspects of bank operations.

[13]FFIEC is composed of the Comptroller of the Currency, one FRS Governor, the OTS Director, the FDIC Chairman, and the Chairman of the NCUA Board.

Table 2: Financial Industry Overview

Regulatory agency	Selected financial service entities for which the agency has primary supervisory or oversight responsibility
Federal Reserve System (FRS)—an independent body composed of 12 reserve banks that supervise and conduct examinations of bank holding companies, their nonbank subsidiaries, and state banks that are members of FRS	state-chartered banks that are members of FRS and their foreign branches and subsidiaries bank holding companies, their nonbank subsidiaries, and their foreign subsidiaries financial holding companies Edge Act corporations U.S. operations of foreign banks payment systems
Federal Deposit Insurance Corporation (FDIC)—a government corporation	state-chartered banks that are not members of FRS federally insured state savings banks
Office of the Comptroller of the Currency (OCC)—a bureau of Treasury	nationally chartered banks and federal branches and agencies of foreign banks
Office of Thrift Supervision (OTS)—a bureau of Treasury	state and federally chartered savings associations savings and loan holding companies
National Credit Union Administration (NCUA)—an independent body	federally chartered credit unions federally insured, state-chartered credit unions corporate credit unions
Securities and Exchange Commission (SEC)—a federal agency	broker-dealers investment advisers investment companies securities exchanges securities clearing agencies National Association of Securities Dealers Municipal Securities Rulemaking Board
state insurance regulators	insurance companies

Source: GAO analysis of data from the above financial services regulators.

Table 3: Banking Regulators Oversee Large, Medium, and Small Institutions

Regulator	Total institutions supervised	Large institutions[a]		Small and medium institutions[b]	
		Number	Assets in billions of dollars	Number	Assets in billions of dollars
FRS	972	25	$1,403	947	$300
FDIC	4,971	13	294	4,958	937
OCC	2,137	42	2,916	2,095	719
OTS	883	17	586	866	377
NCUA	9,984	1	15	9,983	486
Total	**18,947**	**98**	**$5,214**	**18,849**	**$2,819**

Source: GAO analysis of FDIC's *Statistics on Banking* and NCUA data as of December 31, 2001.

[a]$10 billion or more in assets.

[b]Less than $10 billion in assets.

Under Section 111 of the Federal Deposit Insurance Corporation Improvement Act of 1991, each federal banking regulator, with the exception of NCUA, is required to conduct a full-scope, on-site examination of federally insured depository institutions under its jurisdiction at least once during each 12-month period. The act allows for examinations to be extended to 18 months for small (less than $250 million in assets), well-capitalized, well-managed institutions that meet certain criteria. The primary objectives of such examinations of financial institutions, known as safety-and-soundness examinations, are to (1) provide an objective evaluation of the institution's safety and soundness, determine compliance with applicable laws, rules, and regulations; and ensure that it maintains capital commensurate with its risk; (2) appraise the quality and overall effectiveness of management and their risk management systems; and (3) identify, communicate, and follow up in all areas of the examination's recommendations, especially in areas where corrective action is required to strengthen the bank's performance and compliance with laws, rules, and regulations.[14]

The financial institution safety-and-soundness examination assesses six components of a financial institution's performance—capital adequacy,

[14]Other examinations assess the institution's compliance with fair lending and consumer protection laws and the Community Reinvestment Act.

asset quality, management, earnings, liquidity, and sensitivity to market risk. As part of these six components, examiners also consider the adequacy of the financial institution's internal controls, internal and external audit, and compliance with law, in addition to evaluating the institution's management's ability to identify and control risk. Additionally, examiners evaluate the financial institution's use of information technology and third party service providers, including information technology-related servicers.

To assist examiners in assessing information technology risks to plan their examinations, FFIEC developed the Uniform Rating System for Information Technology (URSIT), to provide rating definitions for the information technology examinations of financial institutions and their technology service providers. The URSIT composite rating is considered in the overall management component of the examination. According to FFIEC, the purpose of the rating is to provide a consistent means of evaluating the condition or performance of information technology functions and to provide a mechanism for monitoring those entities whose condition or performance require special supervisory attention. Using URSIT, examiners consider the adequacy of the financial institution's information technology risk management practices; management of information technology resources; and integrity, confidentiality, and availability of automated information. The evaluation of these components can include, but is not limited to, business continuity, information security, network services, change control management, systems development life cycle, audit, internal controls, architecture, vendor management, and board oversight.

SEC's primary mission is to protect investors, maintain the integrity of the securities markets, and oversee the activities of a variety of key market participants. In 2001, SEC was responsible for overseeing 9 exchanges; the over-the-counter market; approximately 70 alternative trading systems, including electronic communication networks;[15] 12 registered clearing agencies; about 8,000 registered broker-dealers employing almost 700,000 registered representatives; almost 900 transfer agents;[16] over 900 investment company complexes; and 7,400 registered investment advisers. In addition, about 14,000 companies that have issued securities have filed annual reports with SEC. SEC's oversight includes rulemaking, surveilling the markets, interpreting laws and regulations, reviewing corporate filings, processing applications, conducting inspections and examinations, and determining compliance with federal securities laws. It is also responsible for regulating public utility holding companies.

Staff within SEC's Market Regulation Division are responsible for examinations of exchanges, clearing organizations, and electronic communication networks. Staff from its Office of Compliance Inspections and Examinations are responsible for examinations of broker-dealers and investment companies. SEC does not directly regulate entities that provide information technology services to firms under its jurisdiction. Broker-dealers and exchanges also operate under rules set by the securities industry's self-regulatory organizations, including the National Association of Securities Dealers and the New York Stock Exchange.

In addition, NAIC assists state insurance regulators in their efforts to protect the interests of insurance consumers. NAIC, which comprises insurance regulators from all 50 states, the District of Columbia, and the four U.S. territories, helps facilitate the regulation of financial and market conduct at the state level.

[15]Alternative trading systems are entities or systems that provide a market place or facility for bringing together purchasers and sellers of securities or otherwise performing functions commonly performed by a stock exchange. Alternative trading systems that offer additional functionality to their customers are known as electronic communication networks.

[16]Transfer agents are parties that maintain records of stock and bond owners.

Cyber Threats Are Increasing, and Infrastructures Are Vulnerable

Increased access to systems created by widespread computer interconnectivity poses significant risks to our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. The speed and accessibility that create the enormous benefits of the computer age likewise, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Table 4 summarizes the key threats to our nation's infrastructures, as observed by the FBI.

Table 4: Threats to Critical Infrastructure Observed by the FBI

Threat	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Information warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence,[a] can affect the daily lives of Americans across the country.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and "worms" have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, and Code Red.

Source: The Federal Bureau of Investigation unless otherwise indicated.

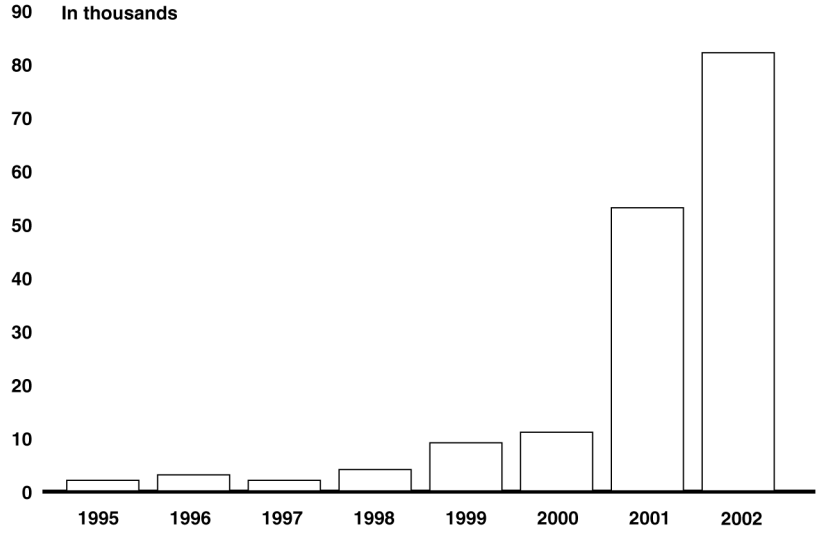
[a]Prepared Statement of George J. Tenet, director of central intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and are using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data. In addition, the disgruntled organization insider is a significant threat, since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions.

The number of computer security incidents reported to the CERT® Coordination Center (CERT®CC)[17] rose from 9,859 in 1999, to 52,658 in 2001, and to 82,094 in 2002. And these are only the reported attacks. The Director, CERT® Centers, stated that as much as 80 percent of actual security incidents goes unreported, in most cases because the organization (1) was unable to recognize that its systems had been penetrated because there were no indications of penetration or attack or (2) was reluctant to report incidents. Figure 1 shows the number of incidents reported to the CERT® CC from 1995 through 2002.

[17]The CERT® Coordination Center (CERT®CC) is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT® Coordination Center: 1995 through 2002



Source: Carnegie-Mellon's CERT® Coordination Center.

According to the *National Strategy for Homeland Security*, terrorist groups are already exploiting new information technology and the Internet to plan attacks, raise funds, spread propaganda, collect information, and communicate securely. The administration's draft *National Strategy to Secure Cyberspace* states that cyber incidents are increasing in number, sophistication, severity, and cost. It further adds that cyber attacks on U.S. information networks occur regularly and can have serious consequences, such as disrupting critical operations, causing loss of revenue and intellectual property, and even causing loss of life.

Since the September 11, 2001, terrorist attacks, warnings of the potential for terrorist cyber attacks against our critical infrastructures have increased. For example, last year the Special Advisor to the President for Cyberspace Security stated in a Senate briefing that although to date none of the traditional terrorist groups, such as al Qaeda, have used the Internet to launch a known attack on the U.S. infrastructure, information on computerized water systems was recently discovered on computers found in al Qaeda camps in Afghanistan. Further, in his October 2001 congressional testimony, Governor James Gilmore warned that systems and services critical to the American economy and the health of our citizens—such as financial services, "just-in-time" delivery systems for goods, hospitals, and state and local emergency services—could all be shut down or severely handicapped by a cyber attack or a physical attack against computer hardware.[18]

Not only is cyber protection of our critical infrastructures important in and of itself, but a physical attack in conjunction with a cyber attack has recently been highlighted as a major concern. In fact, NIPC has stated that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure. As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For example, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack.

Financial Services Sector Faces Cyber Threats

The financial services sector faces cyber threats similar to those faced by other critical infrastructure sectors, but the potential for monetary gains and economic disruptions may increase its attractiveness as a target. Financial services institutions have experienced cyber incidents that have had some impact on their operations, which demonstrates a continuing threat to the industry. Also, the financial services sector is highly

[18]Testimony of Governor James S. Gilmore III, former Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction (commonly referred to as the "Gilmore Commission") before the House Science Committee, Oct. 17, 2001.

dependent on other critical infrastructures. For example, threats facing the telecommunications and power sectors could directly affect the financial services industry. However, after the September 11, 2001, terrorist attacks, the financial markets were able to recover within days, despite significant damage to the World Trade Center area, where a significant concentration of financial entities is located.

Cyber Threats to the Financial Services Sector Exist

According to government and private-sector officials, the financial services sector faces cyber threats similar to those faced by other critical infrastructure sectors. As discussed in the previous section of this report, such threats include attacks from individuals and groups with malicious intent, such as crime, terrorism, and foreign intelligence.

Because it holds over $23.5 trillion in assets, the potential monetary gains and economic disruptions that could occur if the financial services sector's systems were successfully attacked may increase the probability of its becoming a target. For example, a successful widespread cyber attack could erode public confidence in financial institutions, deny businesses and individuals access to their funds, result in the loss of funds, affect the integrity of financial information, or inhibit securities trading. At the same time, sector representatives believe that financial institutions recognize and work to mitigate the threat in order to adhere to federal and state regulations and maintain public confidence in their ability to protect and manage customer assets.

The report of the President's Commission on Critical Infrastructure Protection in 1997 recognized that—on an institutional level, increasing use of electronic banking mechanisms, and perhaps an entirely new infrastructure to accommodate the demand for rapid data recall and payment processing—would create new forms of risk to information systems. Further, regarding the financial services sector, the report of the President's Commission on Critical Infrastructure Protection identified cyber threats to the financial services industry and the corresponding need to improve (1) information sharing between regulators, law enforcement officials, and industry associations; (2) contingency planning through sponsoring strategic simulations and determining the need for additional back-up facilities; (3) examination processes, audit practices, internal controls, and physical security measures to accommodate new kinds of risks and to help deter the insider threat; and (4) information security education and awareness programs within academia and in the general public. The *Banking and Finance Sector: National Strategy for Critical*

Infrastructure Assurance, issued on May 13, 2002, acknowledged that the sector would continue to face physical and cyber threats domestically and internationally. In addition, it stated that cyber threats and vulnerabilities are among the biggest challenges facing the sector, that cyber vulnerabilities and crimes have increased exponentially since the start of the new century, and that this trend will increase in proportion to the reliance placed on technology. Officials from the federal government's NIPC similarly stated that the number of cyber threats faced by the financial services sector has increased. Regarding physical threat, NIPC released an information bulletin in April 2002 warning against possible physical attacks on U.S. financial institutions by unspecified terrorists.[19] The financial services sector's strategy also acknowledged the insider threat, stating that as financial institutions eliminate redundant operations and reduce personnel costs, the reductions can lead to vengeful acts by departing employees, as well as by dissatisfied employees among the remaining staff.

Cyber Vulnerabilities Associated with the Financial Services Sector Have Been Exploited

The financial services sector has been impacted by the successful exploitation of cyber vulnerabilities. For example, the 2002 report of the *Computer Crime and Security Survey*, conducted by the Computer Security Institute and the FBI's San Francisco Computer Intrusion Squad, showed that 90 percent of respondents (primarily large corporations and government agencies, including 19 percent from the financial services sector) had detected computer security breaches within the last 12 months. In addition, 80 percent of respondents acknowledged financial losses due to computer breaches. Respondents willing or able to quantify their financial losses reported losses of over $450 million in total, including over $170 million from the loss of proprietary information and over $115 million from financial fraud.

[19]NIPC, *Possible Terrorism Targeting of US Financial System*, *Information Bulletin 02-003* (Apr. 19, 2002).

A report[20] on Internet security threats by a private-sector managed security firm for the period of January 1, 2002, to June 30, 2002,[21] concluded that companies in the financial services industry, along with energy and high-tech companies, experience the highest rate of attack activity, based on their clients' experience. According to the study, financial service firms received an average of 1,018 attacks per company, and 46 percent of these firms had at least one severe attack during the period studied. Across all industries, the average number of attacks per company was about 788.

The following examples of financial services-related incidents have been publicly reported.

- According to media reports, in 1994, a Russian hacker broke into Citibank's system, stealing $10 million. The company recovered all but $400,000 of that loss, and the case resulted in a felony conviction of the primary hacker.

- In 2000, two men from Kazakhstan were arrested in London for breaking into Bloomberg L.P.'s computer systems in New York in an attempt to extort $200,000 from the firm, according to NIPC and media reports.

Since April 1996, depository institutions have reported to their regulators, through the Suspicious Activity Report System (SARS), any suspicious transactions involving $5,000 or more. The requirement to report computer intrusions through this system started in June 2000. As of May 31, 2002, there have been 656 such filings.[22]

[20]Riptech Incorporated, *Riptech Internet Security Threat Report: Attack Trends for Q1 and Q2 2002, Volume II* (Alexandria, VA.: July 2002).

[21]For the 6-month period, based on information from a sample of its client organizations, Riptech analyzed firewall logs and intrusion detection system alerts. From these initial data, more than 1 million possible attacks were isolated and more than 180,000 confirmed.

[22]FinCen. *The SAR Activity Review: Trends, Tips & Issues*, Issue 4: August 2002.

Interdependencies between Industries Pose Additional Risks to the Financial Services Industry

The financial services industry and the federal government have raised concerns about the financial services sector's interdependency with other critical infrastructures, including telecommunications and energy, and the potential negative impact that attacks in those sectors could have on its ability to operate. Understanding the many interdependencies between sectors is critical to successfully protecting all of our nation's critical infrastructures. According to a January 2001 report by the CIP Research and Development Interagency Working Group,[23] the effect of interdependencies is that a disruption in one infrastructure can spread and appreciably affect other infrastructures.[24] The report also stated that understanding interdependencies is important because the proliferation of information technology has made the infrastructures more interconnected. In congressional testimony in July 2002, the director of Sandia National Laboratories' Infrastructure and Information Systems Center stated that these interdependencies make it difficult to identify critical nodes, vulnerabilities, and optimal mitigation strategies.

According to the financial services sector's national strategy, the industry must take into account the effect of damage from disruptions in other critical sectors, such as telecommunications, electrical power, and transportation. The attacks of September 11, 2001, demonstrated the dependence of the financial services industry on the stability of other sectors' infrastructures. For example, the industry suffered the impact of disrupted communications for its broker-dealers, clearing banks, and other core institutions.[25] The draft *National Strategy to Secure Cyberspace* also discusses the risks posed by interdependent sectors. It states that unsecured sectors of the economy can be used to attack other sectors and that disruptions in one sector have cascading effects that can disrupt multiple parts of the nation's critical infrastructure. Potential vulnerabilities of the telecommunications and energy sectors, two sectors relied upon by the financial services sector, are highlighted next.

[23]The CIP Research and Development Interagency Working Group was established in March 1998 to develop and sustain a roadmap of what technologies should be pursued to reduce vulnerabilities of and counter threats to our critical infrastructures.

[24]CIP Research and Development Interagency Working Group, *Report on the Federal Agenda in Critical Infrastructure Protection Research and Development, Research Vision, Objectives, and Programs*, January 2001.

[25]*Defending America's Cyberspace: Banking and Finance Sector: The National Strategy for Critical Infrastructure Assurance, Version 1.0*, May 13, 2002.

- In February 2002, the National Security Telecommunications Advisory Committee and the National Communications System released a report, *An Assessment of the Risk to the Security of the Public Network*, about the vulnerabilities of the telecommunications sector. This report concluded that (1) the vulnerability of the public network to electronic intrusion has increased, (2) government and industry organizations have worked diligently to improve protection measures, (3) the threat to the public network continues to grow as it becomes a more valuable target and the intruder community develops more sophisticated capabilities to launch attacks against it, and (4) continuing trends in law enforcement and legislation have increased the ability of the government and the private sector to deter the threat of intrusion. The report also stated that the implementation of next-generation network technologies, including wireless technology, and their convergence with traditional networks, have introduced even more vulnerabilities into the public network.

- Energy sector vulnerabilities have also been identified. For example, in October 1997, the President's Commission on CIP reported on the physical vulnerabilities for electric power related to substations, generation facilities, and transmission lines. It further added that the widespread and increasing use of supervisory control and data acquisition (SCADA) systems for controlling energy systems increases the capability of seriously damaging and disrupting them by cyber means. In addition, the previously discussed Internet security threat report also concluded that companies in the energy industry, along with financial services and high-tech companies, experience the highest rate of overall attack activity. According to the study, power and energy firms received an average of 1,280 attacks per company, and 70 percent of them had at least one severe attack during the period studied.

Industry Groups in the Financial Services Sector Have Taken Steps to Improve Information Sharing and Address Threats to Its Infrastructure

Financial services industry groups have taken several steps to address cyber threats and improve information sharing, and they plan to take continuing action to further address these issues. First, industry representatives collaboratively developed a sector strategy—*National Strategy for Critical Infrastructure Assurance*—that discusses additional efforts necessary to identify, assess, and respond to sectorwide threats. However, the financial services sector has not specified how the efforts will be implemented, by providing interim objectives, detailed tasks, timeframes, responsibilities, or processes for measuring progress. Second, FS-ISAC was formed in October 1999 to, among other objectives, facilitate sharing of information and provide its members with early notification of

computer vulnerabilities and attacks. Third, several other industry groups representing the various segments of the financial services sector are taking steps to better coordinate industry efforts and to improve information security across the sector.

Financial Services Sector's National Strategy Identifies Further Needed Actions, but Does Not Provide Detailed Implementation Plans

Industry representatives worked collaboratively on a Treasury-sponsored working group to develop the sector's *National Strategy for Critical Infrastructure Assurance*, which identifies a framework for sector actions—including efforts necessary to identify, assess, and respond to sectorwide threats, including completing a sectorwide vulnerability assessment. In May 2002, Treasury's Assistant Secretary for Financial Institutions submitted the industry's strategy to the Special Advisor to the President for Cyberspace Security, with the understanding that it would provide an evolving baseline for the sector's efforts. The strategy presents a framework for planning and implementing sector action that includes

- analyzing the infrastructure's strengths, interdependencies, vulnerabilities, and abilities to resolve virtual and physical issues and concerns;
- taking steps to strengthen the sector's capacity to prepare for, defend against, and recover financially and technologically from systemic attacks;
- building and implementing strategies for detecting and responding to attacks on the information infrastructure of the financial services sector;
- having the ability to recover and restore technological and financial services and functions to their normal state of operation; and
- having the ability to financially withstand the impact of attacks.

Generally, the strategy discusses the activities called for in PDD 63, as described earlier in this report, including assessing the vulnerabilities of the sector to cyber or physical attack, recommending a plan to eliminate vulnerabilities, proposing a system for identifying and preventing major attacks, and developing a plan for alerting, containing, and rebuffing an attack in progress and then rapidly reconstituting essential operations. In addition, the strategy is generally consistent with the recommendations in the President's Commission report, as discussed earlier in this report,

including addressing (1) a mechanism for information sharing about threats and vulnerabilities; (2) efforts to improve the industry's business continuity planning and ability to recover from disasters, including the need for back-up locations; and (3) actions taken to educate industry executives and information security specialists.

In response to PDD 63's call for a sectorwide vulnerability assessment, the sector's national strategy identifies a number of options for completing an assessment, including (1) with the support of the Department of the Treasury, initiating an effort to identify and assess existing areas of exposure and interdependencies that would pose systemic risk to the banking and finance sector; (2) performing semiannual reviews of the infrastructure for newly identified weaknesses or risks based on technology changes; and (3) evaluating the feasibility of developing and maintaining an industrywide model and simulation process for assessing and addressing the systemic effects of threats to the core infrastructure.

The strategy also states that critical components of the infrastructure must be subject to frequent, rigorous review and assessment of their posture and practices and suggests various approaches to achieve this goal, such as: (1) periodic self-assessments; (2) external assessments and audits of core institutions and/or processes by trusted third parties; (3) formal analysis and assessments of industrywide transaction flows, processes, and procedures in critical areas of service provision; and (4) cross-industry interdependency assessments.

Also, the national strategy for the financial services sector recommends a number of other actions, including

- designing and implementing modeling efforts—business, mathematical, and others—to be used to assess and understand the impact of systemic security issues on the financial services sector;

- developing an awareness campaign for education and outreach to members of the sector, key stakeholders, and boards of directors;

- encouraging the role of insurance and other risk-management techniques to mitigate the impact of a cyber-attack;

- working with government to design and implement a shared coordinated management process for detecting and responding to systemic threats against the infrastructure; and

- exploring funding options to support the sector activities listed above.

According to the strategy, achieving success within this framework will require resources from the entire financial services sector, which must be able to detect, respond to, and recover from cyber and physical infrastructure incidents in a coordinated manner. The strategy goes on to state that this requires a concerted, collaborative effort, not only on the part of the traditional members of the financial services sector and the insurance industry, but also on the part of the sector's vendors, service providers, regulators, and legislators. Moreover, according to the strategy, the financial services sector recognizes that it is not within the capacity of any one individual institution or sector to adequately manage an isolated and independent response to current and future threats.

Although the sector strategy establishes a framework to address CIP efforts, the financial services sector has not developed specific interim objectives; detailed tasks, timeframes, or responsibilities for implementation; or a process for monitoring progress. Without such information, there is an increased risk that the sector's efforts will be unfocused, inefficient, and ineffective. For example, without clearly defined interim objectives and a process for monitoring progress, the success of efforts to complete the sector's actions cannot be measured. Also, establishing detailed tasks and clarifying responsibilities can ensure a common understanding of how the strategy will be implemented, how the actions of organizations are interrelated, who should be held accountable for their success or failure, and whether they will effectively and efficiently support sector goals. The current sector coordinator stated that the recently formed FSSCC plans to review and update the financial services strategy, including consideration of the *National Strategy for Homeland Security* and the draft *National Strategy to Secure Cyberspace*, which were issued subsequent to the financial services sector's strategy. In addition, FSSCC plans to determine what actions the sector needs to take, including the specific interim objectives; detailed tasks, timeframes, or responsibilities for implementation; and a process for monitoring progress to implement the strategy.

Further, the financial services sector's strategy does not discuss the coordination of efforts between the private sector and Treasury as sector liaison or other federal agencies in assessing sector vulnerabilities. According to Treasury officials, the FBIIC vulnerability assessment working group has identified critical entities in the U.S. wholesale financial system and examined the currency production and distribution process. In addition, there are ongoing FBIIC activities to examine other parts of the financial services industry, including the stock and bond markets, commodity futures trading markets, and retail payment systems. Further, FRS, OCC, and SEC (with the participation of the Federal Reserve Bank of New York and the New York State Banking Department) issued a draft white paper on August 30, 2002, that identified certain critical financial markets and proposed sound practices for strengthening the resilience of those markets.[26] However, the strategy does not discuss how these efforts to assess sector vulnerabilities are to be coordinated.

Financial Services Information Sharing and Analysis Center Has Made Progress, but Acknowledges Challenges Concerning Participation and Sharing

In response to PDD 63, the Financial Services ISAC (FS-ISAC) was formed in 1999. A private sector initiative by the banking and finance industry, FS-ISAC is currently composed of 61 members who maintain over 90 percent of the assets under control by the industry, according to FS-ISAC. The mission of FS-ISAC is to use information sharing and analysis to provide its members with a comprehensive set of knowledge resources. These resources include early notification of computer vulnerabilities and attacks and access to subject-matter expertise and other relevant information, such as trending analysis for all levels of management and for first responders to cyber incidents.

[26]Board of Governors of the Federal Reserve System, OCC, and SEC, *Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (Docket No. R-1128: Aug. 30, 2002).

FS-ISAC is a permanently staffed watch center that operates 24 hours a day, 7 days a week. It monitors cyber-related events around the world and acts as a clearinghouse for information that it distributes to its members. According to the current chairperson, FS-ISAC also works with other organizations that have similar missions, including NIPC; the U.S. Secret Service (extensively with the New York Electronic Crimes Task Force);[27] and the Department of Defense's Joint Task Force for Computer Network Operations.[28]

According to its former chairman, FS-ISAC demonstrated its effectiveness as an information dissemination vehicle in the way it handled the ILOVEYOU virus. In May 2000, we highlighted in testimony this example, in which FS-ISAC provided early notification to the industry when it collected reports on the spread of the ILOVEYOU virus and posted an alert to its members several hours before NIPC became aware of the threat.[29] Since that time, according to its former chairman, FS-ISAC has been in the forefront of response to incidents such as Code Red and NIMDA, using its communication capabilities to provide early warning to its members as both viruses began to propagate through the Internet.

According to FS-ISAC's current chairperson, the financial services sector faces a number of challenges regarding the success of FS-ISAC, including how to share more information with the federal government and increase industry participation. Recognizing the need to share information across sectors, the national strategy for the financial services sector states that FS-ISAC should define requirements and processes for exchanging information across sectors. In order to increase the sector's participation,

[27]The New York Electronic Crimes Task Force was formed by the U.S. Secret Service to investigate electronic crimes associated with computer-generated counterfeit currency, counterfeit checks, credit card fraud, telecommunications fraud, access device fraud, and so forth. In addition, the task force has developed educational and training programs to protect children, encouraged research and development of tools and methodologies to prevent crime, supported law enforcement education, and promoted the development of trusted relationships with the public and the private sectors.

[28]The Joint Task Force, Computer Network Operations (JTF-CNO), is the primary Department of Defense organization for coordinating and directing internal activities to detect computer-based attacks, contain damage, and restore computer functionality when disruptions occur.

[29]U.S. General Accounting Office, *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000).

the sector coordinator also has discussed the importance of enhancing FS-ISAC's value to the sector and expanding its membership to include a greater proportion of the sector's members.

In April 2001, we reported that although FS-ISAC received information from NIPC, it had not provided information in return because of reporting incompatibilities and concerns about confidentiality.[30] The sector's national strategy discusses legal impediments to information sharing and public-private partnerships and offers possible solutions, including certain exemptions related to the Freedom of Information Act (FOIA), antitrust, and liability.

The Homeland Security Act of 2002, signed by the President on November 25, 2002, includes provisions that restrict federal, state, and local government use and disclosure of critical infrastructure information that has been voluntarily submitted to the Department of Homeland Security. These restrictions include exemption from disclosure under FOIA, a general limitation on use to critical infrastructure protection purposes, and limitations on use in civil actions and by state or local governments. The act also provides penalties for any federal employee who improperly discloses any protected critical infrastructure information. At this time, it is too early to tell what impact the new law will have on the willingness of the private sector to share critical infrastructure information.

Further, by June 2002, FS-ISAC and NIPC had signed a memorandum of understanding that established a formal agreement for sharing security-related information. This memorandum of understanding encourages information sharing between the two organizations and is designed to facilitate the flow of information between the private sector and the government. The former chairman of FS-ISAC stated that the agreement will enable "a two-way trusted exchange of information in order to analyze and disseminate actionable intelligence on threats, attacks, vulnerabilities, anomalies, and security best practices involving the banking and finance sector." According to NIPC's director, "the information sharing agreement with the FS-ISAC should significantly advance our mutual commitment to our economic security."[31] At the present time, FS-ISAC and NIPC conduct

[30]U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, Apr. 25, 2001).

[31]National Infrastructure Protection Center, Press Release, (June 25, 2002).

bi-weekly threat briefings, according to NIPC officials. The current FS-ISAC chairperson stated that FS-ISAC anticipates signing additional memorandums of understanding with various agencies of the government.

The national strategy for the financial services sector calls for FS-ISAC to work with other associations in developing options to significantly increase participation in information exchange. In response, FS-ISAC is currently developing a "next-generation" model in which it would offer certain information dissemination services to the entire sector. According to the FS-ISAC chairperson, they are exploring various funding methods for this service, including funding by various financial services industry groups or the federal government. In addition, other more expanded services, including best practice development, log correlation and analysis, and threat modeling would be offered.

Several Other Industry Groups Are Taking Steps to Address Cyber Threats

A number of financial services industry groups, including the Financial Services Sector Coordinating Council (FSSCC) and the American Bankers Association (ABA), have taken steps to address cyber threats. These steps are discussed in general in the financial services sector's strategy, including developing product certification programs, disaster recovery programs, and a national strategy for the sector.

FSSCC, organized and chaired by the sector coordinator, held its inaugural meeting on June 19, 2002.[32] Its mission is "to foster and facilitate the coordination of sectorwide voluntary activities and initiatives designed to improve CIP/Homeland Security." To encourage active participation and commitment on the part of member organizations, FSSCC has been created

[32]Current participants include: ABA, America's Community Bankers, American Council of Life Insurers, American Insurance Association, American Stock Exchange, American Society for Industrial Security, Bank Administration Institute, The Bond Market Association, Consumer Bankers Association, Credit Union National Association, Fannie Mae, Futures Industry Association, FS-ISAC, Financial Services Roundtable and BITS, Independent Community Bankers of America, Investment Company Institute, Managed Funds Association, National Automated Clearinghouse Association, National Association of Federal Credit Unions, NASDAQ Stock Market Inc., New York Clearing House, New York Stock Exchange Inc., Securities Industry Association, Security Industry Automation Corporation, and The Options Clearing Corporation. In addition, the sector liaison, Treasury's assistant secretary for financial institutions, who is also the FBIIC Chair, and other FBIIC members, may be invited to attend part of FSSCC meetings to be briefed on council initiatives.

as a limited liability corporation. As part of its efforts, FSSCC established the following objectives:

- provide broad industry representation for CIP and Homeland Security (HLS) and related matters for the financial services sector and for voluntary sectorwide partnership efforts;
- foster and promote coordination and cooperation among the participating sector's constituencies on CIP/HLS related activities and initiatives;
- identify voluntary efforts where improvements in coordination can foster sector preparedness for CIP/HLS;
- establish and promote broad voluntary activities and initiatives within the sector that improve CIP/HLS;
- identify barriers to and recommend initiatives to improve sectorwide voluntary CIP/HLS information, knowledge sharing, and the timeliness of dissemination processes for critical information sharing among all the sector's constituencies; and
- improve sector awareness of CIP/HLS issues, available information, sector activities/initiatives, and opportunities for improved coordination.

One of the council's main initiatives is to share information on CIP activities already being performed by member associations across the entire sector. According to the sector coordinator, FSSCC is targeting relevant trade associations to broaden its membership so that it can reach a greater proportion of the sector's members. It will disseminate information about ongoing CIP activities to this target audience through council members. Furthermore, FSSCC is developing subcommittees and task groups to perform its work. Some of the initial strategic focus areas being considered are:

- information dissemination and information sharing,
- crisis management and response management coordination,
- sector outreach and cross-sector outreach, and

- knowledge sharing—e.g., best practices.

According to FSSCC officials, it has begun working with other private sector entities and with Treasury to coordinate CIP efforts within the sector. In addition, according to the sector coordinator, the establishment of FBIIC provides a strong tool for coordination between the public and private sectors and a forum for financial institution regulators to present a consistent message to the private sector.

The ABA—an industry group whose membership includes community, savings, regional, and money center banks; savings associations; trust companies; and diversified financial holding companies—has an ongoing program for informing its membership of cyber security issues and providing cyber security resources. For example, as a member of FSSCC, ABA is chairing a working group that is responsible for education and outreach initiatives. According to an ABA official, this initiative is designed to inform financial services institutions of existing organizations, including FS-ISAC, which can be used as resources for information regarding physical as well as cyber threats and vulnerabilities. A second aspect of the initiative is to garner feedback from institutions in the financial services sector as to how the process of sharing such information should evolve in terms of organization, services, and cost.

Also in response to cyber security-related issues, ABA created the *Safeguarding Customer Information Toolbox* and made it available in October 2002 to assist ABA members in evaluating their information security and complying with Section 501(b) of the Gramm-Leach-Bliley Act of 1999. In addition, ABA holds interactive webcasts and conferences, distributes a bi-weekly electronic newsletter, the *ABA eAlert*, and provides a variety of resources related to information security through its Web site, at www.aba.com.

BITS[33] is The Technology Group for The Financial Services Roundtable. As part of its mandate, BITS strives to sustain consumer confidence and trust by ensuring the safety and security of financial transactions, and it has several initiatives under way to promote improved information security

[33]BITS is the name of The Technology Group for the Financial Services Roundtable and is not an acronym.

within the financial services industry. BITS's and The Roundtable's membership represents 100 of the largest integrated financial services institutions providing banking, insurance, and investment products and services to American consumers and corporate customers. According to BITS officials, BITS serves as the strategic expert and action-oriented entity for its member companies where commerce, financial services, and technology intersect. According to BITS officials, it is not a lobbying group for the financial services industry.

BITS officials stated that it generally undertakes initiatives for the specific benefit of its member companies, but its efforts often affect the entire financial services industry through its members and through "affiliate" memberships that include other financial services industry groups such as ABA, the Independent Community Bankers of America, and the Credit Union National Association. In addition, most of BITS's work, including best practices, voluntary guidelines, and business requirements, is made public on its Web site at www.bitsinfo.org and shared across the industry. BITS is also an active member of FSSCC, according to BITS officials.

In addition to its work with other financial services industry groups, BITS works with various government agencies, including the President's Critical Infrastructure Protection Board, Office of Cyberspace Security, Office of Homeland Security, CIAO, NIPC, and FBIIC to promote improved information security, best practices for business continuity, and management of relationships with third party service providers.

BITS has a number of working groups on different topics—all of which have a security component.[34] According to BITS, its working groups are made up of experts on the topics from the financial services industry and other participants as appropriate. Each working group has its own set of deliverables, which include self-regulatory requirements, guidelines and self-assessments, and timelines. To set direction and oversee all of BITS's security-related activities, a Security and Risk Assessment Steering Committee (SRA) was established that is made up of the heads of

[34]BITS currently has Working Groups on Aggregation Services, Authentication, Consumer Privacy and Information Use, Crisis Management Coordination, Fraud Reduction, Identity Theft, IT Service Providers, The Role of Insurance in E-Commerce Risk Management, Operational Risk, Patent Issues, Payments Strategies, Security and Risk Assessment, and Standards. In addition to BITS Members, Working Group participants often include regulators, other trade associations, and government agencies.

information security of member organizations. BITS officials' stated priorities include:

- defining and establishing metrics to measure operational risk—working in close coordination with FSSCC, FFIEC, and other regulatory agencies;

- providing security briefings/alerts and government outreach—including regularly sending out alerts to members, establishing an automated alert system for national emergencies, and reaching out to government representatives and other sector and business groups;

- providing, through the BITS Product Certification Program—designed to test products against baseline security criteria—a vehicle to significantly enhance safety and soundness by improving the security of technology products and reducing technology risk;

- issuing the *BITS Framework for Managing Technology Risk for Information Technology (IT) Service Provider Relationships (Framework)*, which includes industry practices and regulatory requirements;

- establishing, with the Roundtable, a crisis management coordination initiative with the overarching objective of improving BITS's member companies' ability to prepare for and recover from significant industrywide disasters; and

- issuing a draft background paper, *Telecommunications for Critical Financial Services: Risks and Recommendations*.

The Securities Industry Association (SIA) also has taken steps to address cyber threats. SIA has more than 600 member securities firms, including investment banks, broker-dealers, and mutual fund companies. According to the sector's national strategy, SIA has a major business continuity planning effort under way to coordinate and develop industry plans for disaster and recovery. According to SIA officials, information about SIA's business continuity planning activities can be found at: http://www.sia.com/business_continuity/.

SIA has also established a virtual command center, which is to be activated when a significant disaster occurs. Before, during, and after such an event occurs, SIA plans for the command center to be the central point for

communicating the status of the disaster and coordinating industry-related response activities for the securities industry. It also intends the command center to act as a liaison between city, state, and federal bodies. In addition, according to SIA, it holds awareness conferences for its member firms and works closely with industry infrastructure organizations, such as exchanges and depositories, and with other industries that its members rely on, such as telecommunications, power utilities, and municipal and state services. SIA is also an active member of FSSCC, through which it shares information with other financial trade associations and regulators through FBIIC.

Sector representatives also identified other industry groups with initiatives related to critical infrastructure protection and information security in the financial services sector, including the following.

- The Financial Services Technology Consortium[35] has had efforts under way since late 2001 involving critical business continuity and disaster recovery. For example, in October 2002, the Consortium initiated with its member financial institutions the development of a shared industry database and clearinghouse to match institutions with available disaster recovery space with those searching for space in a region different than their location. According to a Consortium official, the database will be available in the second quarter 2003. The official also stated that the Consortium's goal is to reduce the time and cost required for financial institutions to find, acquire, and roll out qualified disaster recovery space and added that as a second phase the Consortium will initiate efforts to standardize disaster recovery space and related technologies across the industry. According to a Consortium official, more information is available on its Web site at www.fstc.org.

[35]The Financial Services Technology Consortium is a group of North American-based financial institutions, technology vendors, independent research groups, industry groups, and government agencies that sponsor collaborative technology development in pilots, proof-of-concept, tests, and demonstrations, all supported by member financial institutions and technology companies. According to the Consortium, it aims to bring forward interoperable, open standard technologies that provide critical infrastructures for the financial services industry.

- The Accredited Standards Committee X9, Inc.,[36] develops specific standards related to data and information security for the financial services sector, including standards related to personal identification number management and security, data encryption use by the financial services industry, application of biometrics in banking, wireless financial transaction security, and privacy assessments. According to X9 officials, more information can be found on its Web site at www.x9.org.

Several Federal Entities Play Key Roles in Partnering with the Financial Services Sector on CIP Efforts

Several federal entities play critical roles in partnering with the financial services sector to protect its critical infrastructures. Under PDD 63, Treasury is designated the lead agency for the financial services sector and is responsible for coordinating the public/private partnership between this sector and the federal government. Treasury also chairs the Financial and Banking Information Infrastructure Committee of the President's Critical Infrastructure Protection Board. The committee is responsible for coordinating federal and state financial regulatory efforts to improve the reliability and security of U.S. financial systems. In both of its roles, Treasury has taken steps designed to establish better relationships and methods of communication between regulators, assess vulnerabilities (as discussed earlier in this report), and improve communication 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—such as grants, tax incentives, and regulations—by the federal government to encourage increased private sector participation, as called for in federal CIP policy. In addition to Treasury efforts, other federal CIP-related entities have taken steps to encourage the participation of the financial services sector in CIP.

Treasury Coordinates CIP Efforts Related to the Financial Services Sector

To fulfill Treasury's role in CIP, the Secretary of the Treasury designated the Assistant Secretary for Financial Institutions as the sector liaison for the financial services sector, who works with the sector coordinator—the private sector's focal point for the industry. According to Treasury officials, Treasury strives to ensure that there are open lines of communication

[36]The Accredited Standards Committee X9, Inc., accredited by the American National Standards Institute, develops and publishes voluntary, consensus technical standards for the financial services industry. Its inter-industry voting membership includes over 300 organizations representing investment managers, banks, software and equipment manufacturers, government regulators, and others.

between the government and the private sector and voluntarily participates in industry groups of which Treasury is not an official member. For example, Treasury is involved with groups such as FSSCC, FS-ISAC, and BITS. Treasury also facilitates interaction between CIP Board committees and other government entities involved in CIP and seeks a role in coordinating government and private-sector efforts with the goal of eliminating unnecessary redundancy.

In addition to serving as the sector liaison, Treasury's Assistant Secretary for Financial Institutions also serves as the chair of FBIIC—a standing committee of the President's Critical Infrastructure Protection Board that was established by Executive Order 13231 in October 2001 and was initiated by the Secretary of the Treasury in January 2002. It is charged with coordinating federal and state financial regulatory efforts to improve the reliability and security of U.S. financial systems. Members of FBIIC include representatives of the federal government's financial regulatory agencies as well as state regulators. The committee also works with the sector coordinator to leverage industry initiatives and coordinate private-sector outreach related to CIP.[37] Its members stated that, as part of its responsibilities, FBIIC has initiated a number of efforts. For example, it has initiated a number of working groups on various subjects, including vulnerability assessment, communications, international affairs, and legislative affairs. In addition, FBIIC developed a policy for Government Emergency Telecommunications Service (GETS) cards[38] and is involved in increasing financial institution's participation in the Telecommunications Service Priority (TSP) program.[39] We plan to discuss FBIIC's actions in response to the September 11, 2001, terrorist attacks in further detail in another report requested by this committee.

[37]Department of the Treasury, Press Release, *Treasury Names Private Sector Coordinator for Critical Infrastructure Protection Partnership Effort* (May 14, 2002).

[38]The GETS is a telecommunications service provided by the Office of the Manager, National Communications System, that supports federal, state, and local government, industry, and nonprofit organization personnel in performing their National Security and Emergency Preparedness (NS/EP) missions. It provides emergency access and priority processing in the local and long distance segments of the Public Switched Network. It is to be used in an emergency or crisis situation during which the probability of completing a call over normal or other alternate telecommunication means has significantly decreased.

[39]The TSP Program, developed by the Federal Communications Commission, is used to identify and prioritize telecommunication services that support national security or emergency preparedness missions.

FBIIC also held meetings among the regulatory agencies to share lessons learned about contingency planning operations and created a vulnerability assessment working group. In addition, it is working with the National Communications System[40] and the Federal Communications Commission[41] on telecommunications reliability and developing secure communication methods for regulatory agencies. Further, FBIIC representatives participate in private-sector professional conferences and seminars to promote CIP. Treasury and regulatory agency officials stated that a constructive relationship has been developed between Treasury, the regulators, and the financial services sector because of the mutual, long-standing efforts to improve the financial services industry and the assistance provided by the regulators when crises occur—such as during natural disasters.

Treasury Has Not Undertaken a Comprehensive Assessment of the Use of Public Policy Tools

PDD 63 stated that sector liaisons should identify and assess economic incentives, such as public policy tools—grants, tax incentives, or regulation—to encourage desired CIP behavior in the sector. It further stated that "the incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people." The *National Strategy for Homeland Security* reiterated the need to use all available policy tools to raise the security of the nation's critical infrastructures. It discussed the possible need for incentives for the private sector to adopt security measures or invest in improved safety technologies. It also stated that the federal government will need to rely on regulation in some cases. In addition, the national strategy for the financial services sector recognized that the sector needs to explore funding options to support its activities.

[40]In 1963, the National Communications System was established by presidential memorandum as a federal interagency group responsible for the national security and emergency preparedness telecommunications. These responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure, which now includes the Internet, to achieve effectiveness in managing and using national telecommunication resources to support the federal government during any emergency.

[41]The Federal Communications Commission (FCC) is an independent U.S. government agency. FCC, established by the Communications Act of 1934, is charged with regulating interstate and international communications by radio, television, wire, satellite, and cable. FCC's jurisdiction covers the 50 states, the District of Columbia, and U.S. possessions.

According to a Treasury official, the department has not undertaken a comprehensive assessment of the potential use of public policy tools to encourage the financial services sector in implementing CIP-related efforts. Treasury has instead focused on what it considers to be more important priorities, including establishing better relationships and methods of communication between regulators, performing vulnerability assessments, and establishing GETS policy. Without appropriate consideration of public policy tools, private sector participation in sector-related CIP efforts may not reach its full potential.

Different models are being used in other critical infrastructure protection sectors for funding CIP activities. For example, the Environmental Protection Agency reported providing 449 grants to assist large drinking water utilities in developing vulnerability assessments, emergency response/operating plans, security enhancement plans and designs, or a combination of these efforts. In a different approach, the American Chemistry Council requires members to perform enhanced security activities, including vulnerability assessments.

Other Federal Entities Play Key Roles

Other federal CIP entities coordinate with the financial services sector. For example, NIPC coordinates the efforts of the ISACs, including FS-ISAC. According to NIPC officials, the memorandum of understanding has already led to increased information sharing between NIPC and FS-ISAC. These officials informed us that most of the information sharing agreements with the ISACs contain cyber and physical incident reporting thresholds specific to the industry. In response to our previous recommendations, these officials also told us that a new ISAC development and support unit had been created, whose mission is to enhance cooperation and trust between the public and private sectors, resulting in a two-way sharing of information.

In addition, the Department of Commerce's CIAO is involved with outreach and education programs in the private sector. Because it is a national organization, CIAO covers the financial services sector as only one component of the nation's critical infrastructure. CIAO officials stated that it is important to include financial services representatives in as many CIP activities as possible. CIAO works in part with the financial services sector to educate the public and raise its awareness of and participation in CIP efforts and to integrate infrastructure assurance objectives into both the public and private sectors.

Finally, as previously mentioned, the President's Special Advisor for Cyberspace Security chairs the Critical Infrastructure Protection Board and works closely with the federal government and the private sector to coordinate protection of the nation's critical infrastructure information systems, including those in the financial services industry. The Special Advisor is also tasked with coordinating intergovernmental agency efforts to secure information systems. Several officials from the financial services sector told us that the Special Advisor has taken an active role in promoting governmental partnership efforts, enjoys a strong relationship with the financial services sector, and advocates initiatives sponsored by the private sector, such as BITS's Product Certification Program.

Federal Regulators Have Taken Steps to Address Information Security Issues

Federal regulators have taken several steps to address information security issues. These steps include consideration of information security risks in determining the scope of their examinations of financial institutions, development of guidance for examining information security and for protecting against cyber threats, and reviewing the practices of information technology service providers.

Regulators have historically played a role in the oversight of the financial services sector. As part of that oversight, financial institution regulators and SEC have generally considered information security risks in determining the scope of their examinations. The purposes of such risk-based examinations vary and may not be specifically focused on critical infrastructure protection. For example, safety and soundness examinations of financial institutions include evaluating compliance with laws such as section 501(b) of the Gramm-Leach-Bliley Act. SEC's examinations of securities exchanges, clearing organizations, and certain electronic communication networks are intended to determine whether they comply with SEC's voluntary guidance, the Automation Review Policy program. The program is focused on certain operational issues, including information technology, of which information security is a part. SEC's examinations of broker-dealers' information technology were initiated in July 2001 as a result of the Gramm-Leach-Bliley Act. These examinations are targeted at the adequacy of safeguards against unauthorized disclosure of customer information.

In addition, the nature and scope of information security evaluations at regulated entities varies. Regulators determine the scope of examinations through risk analysis and the examiner's judgment. Consequently, because information security is considered in relation to other areas in determining

the scope of the examination, it may receive only a limited review. Because we did not review bank examinations as part of our scope on this review, we were unable to independently determine how often and how extensively regulatory agencies reviewed information security at the entities they oversee.

Nonetheless, through examinations, regulators obtain information about the adequacy of information security at certain individual financial institutions, which can be used to suggest improvements where appropriate. The nature and extent of such information varies and, according to a Treasury official, examinations are not integrated with the federal government's CIP efforts. According to FFIEC officials, examinations by the FFIEC agencies—and their results—are confidential by law, and are therefore not shared between FFIEC member agencies or with non-FFIEC member agencies. For example, according to the Federal Reserve, information sharing is limited by banking laws, trade secret laws, and the Federal Reserve's regulations. As discussed earlier in this report, Treasury has not undertaken a comprehensive assessment of the potential use of public policy tools, such as grants, tax incentives, and regulations (including regulations related to examinations). However, the *National Strategy for Homeland Security* reiterated the need to use all available policy tools to raise the security of the nation's critical infrastructures.

Other actions are being taken by regulators to address information security. FFIEC is in the process of updating its Information Systems Examination Handbook, which provides regulators with general guidance on information systems and other areas of technology examinations, such as business continuity, information security, electronic banking, vendor management, payment systems, and audit. Also, as discussed earlier in this report, FRS, OCC, and SEC (with the participation of the Federal Reserve Bank of New York and the New York State Banking Department) issued a draft white paper on August 30, 2002, that identified certain critical financial markets and proposed sound practices for strengthening the resilience of those markets. In addition, the regulators have issued over the years numerous guidance documents regarding information security. For example, in 2001, FFIEC agencies issued detailed enforceable guidelines to carry out the requirements set forth in Section 501(b) of the Gramm-Leach-Bliley Act regarding the safeguarding of customer information by insured depository institutions.

We plan to discuss related actions taken by the regulators in response to the September 11, 2001, terrorist attacks in further detail in another report requested by this committee.

Conclusions

The computer interconnectivity used by the financial services sector for customer services and operations poses significant information security risks to computer systems and to the critical operations and infrastructures they support. Moreover, the dependence of the financial services sector on other critical infrastructures poses additional risk. Industry groups in the financial services sector have taken several steps to share information on cyber threats and to address these threats, including developing a sector strategy. The strategy identifies a framework for sector actions necessary to identify, assess, and respond to sectorwide threats, including completing a sectorwide vulnerability assessment. However, the financial services industry has not developed detailed interim objectives; detailed tasks, timeframes, or responsibilities for implementation; or processes for measuring progress in implementing the sector's strategy.

Federal entities have taken a number of steps to coordinate federal government and private-sector efforts and to assist the financial services sector in its CIP effort, but Treasury has not undertaken a comprehensive assessment, as called for in federal CIP policy, of the potential use of public policy tools to encourage increased sector participation. Consideration of the need for public policy tools is important to encouraging private sector participation in sector-related CIP efforts, including implementation of the sector's strategy. Finally, federal regulators have taken several steps to address information security issues, including 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.

Recommendations for Executive Action

To improve the likelihood of success of the financial services sector's CIP efforts, we recommend that the Secretary of the Treasury direct the Assistant Secretary for Financial Institutions, the banking and finance sector liaison, to coordinate with the industry in its efforts to update the sector's *National Strategy for Critical Infrastructure Assurance* and in establishing interim objectives, detailed tasks, timeframes, and responsibilities for implementing it and a process for monitoring progress. As part of these efforts, the Assistant Secretary should assess the need for

grants, tax incentives, regulation, or other public policy tools to assist the industry in meeting its goals.

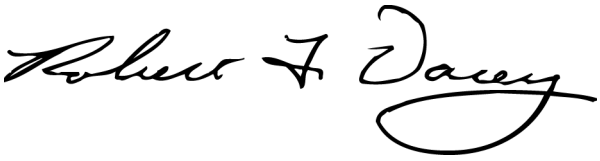
Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Department of the Treasury and the Securities and Exchange Commission (see apps. II and III, respectively). In Treasury's response, the Assistant Secretary for Financial Institutions highlighted the department's efforts to meet its CIP responsibilities. In addition, he recognized the need to continue to work with the sector to increase its resiliency, including consideration of appropriate incentives. In the Securities and Exchange Commission response, the Director of the Division of Market Regulation and the Director of Compliance Inspections and Examinations stated that they look forward to working with Treasury to implement the recommendations.

We also received technical comments from the Federal Deposit Insurance Corporation, the FBI's National Infrastructure Protection Center, the Federal Reserve, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission. In addition, we received written and oral technical comments from ABA, BITS, FS-ISAC, FSSCC, the Financial Services Sector Coordinator, and SIA. Comments from all of these organizations have been incorporated into the report, as appropriate. The Department of Commerce's CIAO, Office of Thrift Supervision, and the National Credit Union Association reviewed a draft of the report and had no comments.

As we agreed with your staff, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies of this report to other interested congressional committees and the heads of the agencies discussed in this report, as well as the private-sector participants and other relevant agencies. In addition, this report will be available at no charge on our Web site at http://www.gao.gov.

If you or your offices have any questions about matters discussed in this report, please contact me at (202) 512-3317 or Michael Gilmore at (202) 512-9374. We can also be reached by e-mail at daceyr@gao.gov or gilmorem@gao.gov, respectively. Key contributors to this report are listed in appendix IV.



Robert F. Dacey
Director, Information Security Issues

Objectives, Scope, and Methodology

Our objectives were to identify the (1) 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) 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. To accomplish these objectives, we reviewed relevant documents, policy, and directives and interviewed pertinent officials from federal agencies and the private sector involved in efforts to enhance the security of the financial services industry.

To determine the general nature of the cyber threats faced by the financial services industry, we reviewed relevant reports, such as the 1997 report of the President's Commission on Critical Infrastructure Protection and the sector's strategy, *Defending America's Cyberspace: Banking and Finance Sector: The National Strategy for Critical Infrastructure Assurance*, *Version 1.0*, May 13, 2002. We also reviewed documentation or interviewed officials from industry groups, including the American Bankers Association (ABA), the BITS Technology Group, the Financial Services Information Sharing and Analysis Center (FS-ISAC), and the Financial Services Sector Coordinating Council (FSSCC). In addition, we held discussions with officials at the Department of Commerce's Critical Infrastructure Assurance Office (CIAO), the National Infrastructure Protection Center (NIPC) at the Federal Bureau of Investigation (FBI), the Department of the Treasury's Office of the Assistant Secretary for Financial Institutions, the Federal Financial Institutions Examinations Council (FFIEC) and its member agencies, the Financial and Banking Information Infrastructure Committee (FBIIC), and the Securities and Exchange Commission (SEC), among others.

To determine the steps the financial services industry has taken to share information on and to address threats, vulnerabilities, and incidents, we reviewed relevant sectorwide documents, such as the sector's strategy, *Defending America's Cyberspace: Banking and Finance Sector: The National Strategy for Critical Infrastructure Assurance*, *Version 1.0*, May 13, 2002, and documents from industry groups, such as FSSCC and FS-ISAC. We also held discussions with the banking and finance sector coordinator, ABA, and BITS.

To determine the relationship between government and private sector efforts to protect the financial services industry's critical infrastructures, we reviewed relevant documents, including prior GAO reports and

testimonies, and held discussions with federal officials from CIAO, NIPC, the Department of the Treasury's Office of the Assistant Secretary for Financial Institutions, FFIEC, FBIIC, and SEC. In addition, we interviewed officials from industry groups, including ABA and BITS, as well as the banking and finance sector coordinator.

To determine the actions financial regulators have taken to address these cyber threats, we reviewed relevant reports, guidelines, and policies, such as FFIEC's Information Systems Examination Handbook. We also interviewed officials from the Treasury's Office of the Assistant Secretary for Financial Institutions, FFIEC, FBIIC, SEC, and the Board of Governors of the Federal Reserve System.

We performed our work in Washington, D.C., from July to November 2002 in accordance with generally accepted government auditing standards. We did not evaluate the frequency or extent of examinations performed by the federal regulators or SEC.

Comments from the Department of the Treasury

ASSISTANT SECRETARY

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

January 23, 2003

Mr. Robert F. Dacey
Director, Information Security Issues
General Accounting Office
Washington, DC

Dear Mr. Dacey:

Thank you for the opportunity to review GAO's report, "Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats." Much progress has been made in ensuring the resiliency of the financial sector during the past several years, but much work remains. In these comments, I wish to amplify on the report's description of the Department's role in and approach to critical infrastructure protection within the financial sector, particularly going forward.

The Treasury has always played a critical role in strengthening the ability of the financial sector to withstand disruptions of all types, including foreign debt crises, natural disasters, stock market declines, and the failure of financial institutions. In the area of critical infrastructure protection, however, our responsibility has been more formally assigned, namely, through two separate, but related, directives.

First, the U.S. Treasury Department was assigned lead agency responsibility for the banking and finance sector with regard to critical infrastructure protection by Presidential Decision Directive 63 (PDD 63), which was issued in 1998. The Department received additional responsibility as a result of President Bush signing Executive Order 13231, "Critical Infrastructure Protection in the Information Age," on October 16, 2001, which established the President's Critical Infrastructure Protection Board and the Financial and Banking Information Infrastructure Committee (FBIIC). This executive order directed the Treasury Department to chair FBIIC and lead the development of its mission and strategic plan. We note that the National Strategy for Homeland Security issued by the Office of Homeland Security reiterated PDD 63's assignment of Treasury as the lead agency for the banking and finance sector in matters concerning critical infrastructure protection and homeland security.

The Department has worked proactively to meet the responsibilities assigned to us by PDD 63 and the Executive Order and has deliberately established a phased, four-stage approach to: (1) form a public/private partnership; (2) organize the public sector; (3) facilitate the organizing of the private sector; and (4) identify public efforts that would further the resiliency of the sector, such as subsidies, regulations, best practices, and legislation, among other measures. We have found success in proceeding so as to keep the horse before the cart and ensuring that the federal government is as prepared as we are asking the private sector to be.

The Public/Private Partnership

Recognizing that the private sector owns and operates the overwhelming majority of the financial sector's critical infrastructure, we determined that we could only protect that infrastructure cooperatively, in partnership with industry. In accordance with PDD 63, we initially focused on information sharing, research and development, education and outreach, and vulnerability assessments. The most notable product of this approach came in the area of information sharing. In 1999, the financial industry joined together to form the Financial Services Information Sharing and Analysis Center (FS/ISAC) – a testament to private sector commitment to this issue.

The partnership itself has been the most important result of PDD 63, constituting the means by which we have been able to work closely with industry on matters of critical infrastructure protection. Implementing the other stages of our approach has been made easier and more effective because of the partnership.

Organizing the Public Sector

Immediately after the attacks of September 11, many separate and unrelated efforts to evaluate the resiliency of the financial sector were instituted. Treasury reacted by contacting the federal financial regulators and worked with them to identify systemic vulnerabilities and strategies required for their mitigation. We also realized that the numerous disparate efforts would have to be centralized or the partnership with industry would be jeopardized, as the federal government and its consultants peppered industry with redundant requests for information, meetings, and actions. Moreover, cyber and physical threats were being addressed separately, thus leading to the same inefficiencies.

We sought to address these concerns by coordinating federal involvement with the financial sector within FBIIC. To this end, we invited broad participation from state regulatory organizations and federal financial regulators, the Office of Homeland Security, and the Office of Cyberspace Security. In cooperation with these entities, we have worked to ensure that the public sector got its own affairs in order as we asked the private sector to follow our lead. Thus, we addressed public sector preparedness for physical or cyber attacks. For example, FBIIC sponsored continuity of operations efforts and developed emergency communication protocols for member agencies.

We have also continued to examine critical financial assets and assess their vulnerabilities. Treasury is currently in the process of reviewing the FBIIC vulnerability assessments to identify any gaps not yet identified and offer mitigation strategies in partnership with the private sector.

Assisting the Organization of the Private Sector

After making sufficient progress with FBIIC and given our productive partnership with industry, we appointed a sector coordinator and charged that person with the task of organizing the private sector. This led to the formation of the Financial Services Sector Coordinating

Council, whose members include the major financial services trade associations and the financial utilities. The Council is working on such issues as ensuring that the FS/ISAC continues to play a vital role within the sector, improving mechanisms by which important information can be shared with the relevant parties as quickly as possible, and the process by which the sector can respond to and communicate during a crisis.

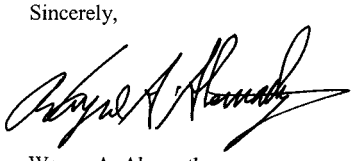
Public Policy Initiatives

These initial efforts have built a foundation upon which we can take further measures to mitigate risks and respond to challenging events. With that experience and base of knowledge in place, Treasury continues to evaluate requests for financial assistance from a variety of sources. Treasury also participates in an Office of Homeland Security working group that is considering the merits of various public policy mechanisms for achieving resiliency across sectors.

As the process continues to evolve from evaluating vulnerabilities and mitigation approaches to an increasingly greater focus on private sector implementation of mitigation strategies, we are relying on the strength of our partnership for both cooperation and insight into how this effort can best succeed. We believe that regulation should be considered as a last resort, used as a tool in our cooperative efforts. Moreover, legislative improvements can best be identified within the context of a trusted partnership.

I believe both the public and private sector have made great strides in improving our ability to prevent, prepare for, and respond to physical or cyber attacks against the financial system. I am pleased that the GAO is highlighting these successes, and the Department looks forward to continuing to work with all relevant parties to ensure the resiliency of the financial sector.

Sincerely,



Wayne A. Abernathy
Assistant Secretary for Financial Institutions

Comments from the Securities and Exchange Commission

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

January 10, 2003

Mr. Robert F. Dacey
Director, Information Security Issues
United States General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Dacey:

This letter responds to your request to review and comment on the draft Report entitled Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats, GAO-03-173. We appreciate the opportunity to comment on this Report.

The GAO recommends that the Secretary of the Treasury direct the Assistant Secretary for Financial Institutions, the banking and finance sector liaison, to coordinate with the industry in establishing interim objectives, detailed tasks, timeframes, and responsibilities for implementing the sector's National Strategy for Critical Infrastructure Assurance and a process for monitoring progress. As part of these efforts, the GAO recommends that the Assistant Secretary assess the need for grants, tax incentives, regulation, or other public policy tools to assist the industry in meeting its goals.

We look forward to working with Treasury to implement this recommendation.

* * *

Thank you again for the consideration that you and your staff have shown to our staff and the opportunity to comment on this draft Report. Please contact us if it would be useful for us to elaborate on this letter.

Sincerely,

Annette L. Nazareth
Director
Division of Market Regulation

Lori A. Richards
Director
Office of Compliance Inspections and Examinations

GAO Contact and Staff Acknowledgments

GAO Contact

Robert Dacey (202) 512-3317

Acknowledgments

Key contributors to this report include Michael Gilmore, Cody Goebel, Joanne Fiorino, Dave Hinchman, Daniel Hoy, Nick Marinos, James McDermott, Dave Powner, Jamelyn Smith, and Karen Tremba.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to GAO Mailing Lists" under "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00