

GAO

Report to the Committee on Financial
Services, House of Representatives

February 2003

POTENTIAL TERRORIST ATTACKS

Additional Actions Needed to Better Prepare Critical Financial Market Participants



GAO
Accountability • Integrity • Reliability

Highlights

Highlights of [GAO-03-414](#), a report to the Committee on Financial Services House of Representatives

Why GAO Did This Study

September 11 exposed the vulnerability of U.S. financial markets to wide-scale disasters. Because the markets are vital to the nation's economy, GAO assessed (1) the effects of the attacks on market participants' facilities and telecommunications and how prepared participants were for attacks at that time, (2) physical and information security and business continuity plans market participants had in place after the attacks, and (3) regulatory efforts to improve preparedness and oversight of market participants' risk reduction efforts.

What GAO Recommends

GAO recommends that the Chairman, SEC, work with industry to

- develop goals and strategies to resume trading in securities markets,
- determine sound business continuity practices needed to meet these goals,
- identify organizations critical to market operations and ensure they implement sound business continuity practices, and
- test strategies to resume trading.

In addition, the report contains recommendations to improve SEC's oversight of information technology issues.

www.gao.gov/cgi-bin/getrpt?GAO-03-414.

To view the full report, including the scope and methodology, click on the link above. For more information, contact Davi M. D'Agostino (202) 512-8678 or dagostinod@gao.gov.

POTENTIAL TERRORIST ATTACKS

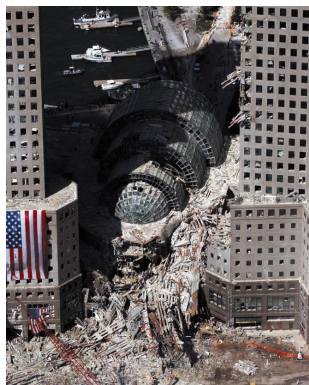
Additional Actions Needed to Better Prepare Critical Financial Market Participants

What GAO Found

The September 11 attacks severely disrupted U.S. financial markets, resulting in the longest closure of the stock markets since the 1930s and severe settlement difficulties in the government securities market. While exchange and clearing organization facilities were largely undamaged, critical broker-dealers and bank participants had facilities and telecommunications connections damaged or destroyed. These firms and infrastructure providers made heroic and sometimes ad hoc and innovative efforts to restore operations. However, the attacks revealed that many of these organizations' business continuity plans (BCP) had not been designed to address wide-scale events.

GAO reviewed 15 organizations that perform trading or clearing and found that since the attacks, these organizations had improved their physical and information security measures and BCPs to reduce the risk of disruption from future attacks. However, many of the organizations still had limitations in their preparedness that increased their risk of being disrupted. For example, 9 organizations had not developed BCP procedures to ensure that staff capable of conducting their critical operations would be available if an attack incapacitated personnel at their primary sites. Ten were also at greater risk for being disrupted by wide-scale events because 4 organizations had no backup facilities and 6 had facilities located between 2 to 10 miles from their primary sites.

The financial regulators have begun to jointly develop recovery goals and business continuity practices for organizations important for clearing; however, regulators have not developed strategies and practices for exchanges, key broker-dealers, and banks to ensure that trading can resume in a timely manner in future disasters. Individually, SEC has reviewed exchange and clearing organization risk reduction efforts, but had not generally reviewed broker-dealers' efforts. The bank regulators that oversee the major banks had guidance on information security and business continuity and reported examining banks' risk reduction measures annually.



An aerial view on September 17, 2001, shows the debris-clogged Winter Garden between the buildings of the World Financial Center near the World Trade Center, which collapsed following the September 11 terrorist attack. These surrounding buildings, which contained important facilities of various financial market participants, were heavily damaged by the debris and massive force of the falling twin towers.

Source: Associated Press.

Contents

Transmittal Letter	1
Executive Summary	3
Purpose	3
Results in Brief	4
Principal Findings	9
Recommendations	16
Agency Comments and GAO Evaluation	16
Chapter 1	18
Introduction	18
Various Organizations Participate in Stock and Options Markets	18
Government Securities and Money Market Instruments Are Traded Differently from Stocks	20
Payment Systems Processors Transfer Funds for Financial Markets and Other Transactions	22
Certain Market Participants Are Critical to Overall Functioning of the Securities Markets	22
Various Regulators Oversee Securities Market Participants, but Approaches and Regulatory Goals Vary	23
Telecommunications and Information Technology Are Vital to Securities Markets	24
Financial Organizations Manage Operations Risks by Protecting Physical and Information Security and Business Continuity Planning	25
Objectives, Scope, and Methodology	25
Chapter 2	29
September 11 Attacks Severely Disrupted U.S. Financial Markets	29
Attacks Caused Extensive Damage and Loss of Life and Created Difficult Conditions That Impeded Recovery Efforts	29
Damage from Attacks Significantly Disrupted Telecommunications and Power	37
Attacks Severely Affected Financial Markets but Heroic Efforts Were Made to Restore Operations	44
Disruptions in Government Securities and Money Markets Severely Affected Clearance and Settlement, Liquidity, and Trade Volumes	48
Impact of Attacks on the Banking and Payments Systems Was Less Severe	53

	Attacks Revealed Limitations in Financial Market Participants’ Business Continuity Capabilities	55
	Observations	57
Chapter 3		58
Financial Market Participants Have Taken Actions to Reduce Risks of Disruption, but Some Limitations Remain	In Climate of Increasing Risk, Organizations Often Have to Choose How to Best Use Resources	58
	All Financial Market Organizations Were Taking Steps to Reduce the Risks of Operations Disruptions	62
	Some Financial Organizations Had Preparedness Limitations That Increased Their Risk of an Operations Disruption	63
	Observations	67
Chapter 4		68
Financial Market Regulators Lack Recovery Goals for Trading and Could Strengthen Their Operations Risk Oversight	Regulators Are Developing Recovery Goals and Sound Business Continuity Practices for Clearing Functions but Not for Trading Activities	69
	Program, Staff, and Resource Issues Hamper SEC Oversight of Market Participants’ Operations Risks	73
	Bank Regulators Have Authority to Oversee Operational Risk	82
	Conclusions	84
	Recommendations	87
	Agency Comments and Our Evaluation	87
Appendixes		
Appendix I: Telecommunications Providers and Others Cooperated to Overcome Damage to Telecommunications Infrastructure		90
	The Terrorist Attacks Extensively Damaged Local Telecommunications Infrastructure	90
	Telecommunications Carriers and Government Agencies Worked Together to Overcome Challenges	93
Appendix II: Regulator and Market Participants Are Working to Improve Crisis Response and Telecommunications Resiliency		97
	New Organizations Will Increase the Extent to Which Critical Infrastructure Protection Efforts Address the Financial Sector	97
	Regulators and Market Participants Are Acting to Improve Crisis Response	98

	Numerous Initiatives Are Under Way to Strengthen the Resiliency of Local Telecommunications Services	100
Appendix III:	Comments from Federal Reserve System	108
Appendix IV:	Comments from the Securities and Exchange Commission	109
Appendix V:	GAO Contacts and Staff Acknowledgments	111
	GAO Contacts	111
	Acknowledgments	111

Figures

Figure 1:	Clearance and Settlement Process for Stocks	20
Figure 2:	Buildings Destroyed or Damaged on September 11, 2001	30
Figure 3:	Geographic Extent of Damage and Debris from Attacks in Lower Manhattan	32
Figure 4:	Damage to Buildings from Attacks and Resulting Debris	33
Figure 5:	Dust and Debris Resulting from Attack	34
Figure 6:	Lower Manhattan Area Subject to Access Restrictions Following September 11, 2001, Attacks	36
Figure 7:	Damage to Verizon Central Office at 140 West Street	38
Figure 8:	Area Served by Verizon 140 West Street Central Office	40
Figure 9:	Verizon Used Temporary Cabling Solutions at 140 West Street	43
Figure 10:	Failed Transactions in the Government Securities Markets During September 2001	50
Figure 11:	Cash Purchases of Government Securities and Repo Market Activity During September 2001	51
Figure 12:	Intervals between Most Recent SEC ARP Examinations of Critical Exchanges and Clearing Organizations	79
Figure 13:	Verizon Overcame Major Challenges During 140 West Street Restoration Efforts	95
Figure 14:	The SFTI Network Provides Redundant Connections	105

Abbreviations

Amex	American Stock Exchange
ARP	Automation Review Policy
BCP	Business Continuity Plan
BNet	Business Network of Emergency Resources
BONY	Bank of New York
CHIPS	Clearing House Inter-bank Payments System
DOITT	Department of Information Technology and Telecommunications
ECN	Electronic Communications Network
FBIIC	Financial and Banking Information Infrastructure Committee
FCC	Federal Communications Commission
FISCAM	Federal Information System Controls Audit Manual
FRBNY	Federal Reserve Bank of New York
GETS	Government Emergency Telecommunications Service
GLBA	Gramm-Leach-Bliley Act
GSCC	Government Securities Clearing Corporation
IDB	Inter-Dealer Broker
MARC	Mutual Aid and Restoration Consortium
NCS	National Communications System
NRIC	National Reliability and Interoperability Council
NSCC	National Securities Clearing Corporation
NYSE	New York Stock Exchange
OCC	Office of the Comptroller of the Currency
OCIE	Office of Compliance, Inspections, and Examinations
PBX	Private Bank Exchange
SEC	Securities and Exchange Commission
SFTI	Secure Financial Transaction Infrastructure
SIA	Securities Industry Association
SIAC	Securities Industry Automation Corporation
SONET	Synchronous Optical Network
SRO	Self-Regulatory Organization
TSP	Telecommunications Service Priority

This is a work of the U.S. Government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. It may contain copyrighted graphics, images or other materials. Permission from the copyright holder may be necessary should you wish to reproduce copyrighted materials separately from GAO's product.



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

February 12, 2003

The Honorable Michael Oxley, Chairman
The Honorable Barney Frank, Ranking Minority Member
The Honorable Paul E. Kanjorski
Committee on Financial Services
House of Representatives

This report presents the results of the review you requested on the preparations that financial markets have made since the September 11, 2001, terrorist attacks to protect themselves from physical and electronic attacks and to develop business continuity plans for recovering rapidly and resuming operations if damage occurs. The massive destruction caused by the attacks on the World Trade Center and the resulting loss of life, facilities, telecommunications, and power significantly affected U.S. financial markets. The markets reopened within days despite enormous obstacles, but the attacks also exposed the vulnerability of the financial markets to disruption by such events. In conducting this work, we assessed:

the effects of the attacks on the facilities and telecommunications services of participants in the stock and option markets, the markets for government securities and money market instruments, and the banking and payments systems and how prepared market participants were for the attacks at that time;

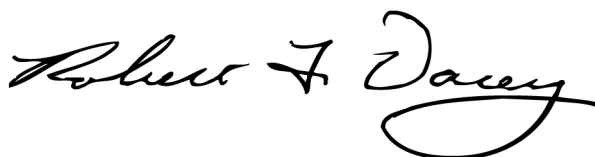
1. the physical and information security and business continuity measures 15 exchanges, clearing organizations, electronic communication networks, and payment system processors had in place after the attacks to reduce the risk of operations disruptions in the future; and
2. the financial regulators' oversight of market participants' efforts to reduce their operations risks and regulatory efforts under way to better prepare the markets for future attacks.
3. This report contains recommendations to the Chairman, Securities and Exchange Commission (SEC) designed to better ensure that U.S. securities markets are better prepared to recover from future disasters. The report also contains recommendations to improve SEC's oversight of information technology issues.

As we agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. We will then send copies to the

secretary, Treasury; the Chairman, SEC; the Chairman, Federal Reserve; and the Comptroller of the Currency; and others who request them.



Davi M. D'Agostino
Director, Financial Markets
and Community Investment



Robert F. Dacey
Director, Information Security



Linda Koontz
Director, Information Management



Keith Rhodes
Chief Technologist
Director, Center for Technology
and Engineering

Executive Summary

Purpose

The massive destruction caused by the September 11, 2001, terrorist attacks on the World Trade Center and the resulting loss of life, facilities, telecommunications, and power significantly affected U.S. financial markets, which were concentrated in lower Manhattan. Despite enormous obstacles, the markets for stocks, options, government securities, and money market instruments all had reopened by the following week, but the attacks also exposed the vulnerability of the financial markets to disruption by such events.¹ Because the markets are vital to the nation's economy, congressional requesters asked GAO to review preparations that financial markets have made since the attacks to protect themselves from physical and electronic attacks and the business continuity plans (BCP) that describe the resources and procedures they would use to recover and resume operations if damage occurs. GAO assessed (1) the effects of the attacks on the facilities and telecommunications services of participants in the stock and option markets, the markets for government securities and money market instruments, and the banking and payment systems and how prepared market participants were for the attacks at that time; (2) the physical and information security and business continuity measures 15 market organizations had in place after the attacks to reduce the risk of operations disruptions in the future; and (3) joint regulatory efforts to better prepare the markets for future attacks and individual financial regulators' oversight of market participants' efforts to reduce their operations risks.

In performing its work, GAO reviewed regulatory and industry documents and studies and interviewed staff from broker-dealer and bank participants, regulators, infrastructure providers, industry associations, and others to determine the impact of the attacks and the preparedness of market participants at the time. To determine security and business continuity measures that 15 financial market organizations had in place to prevent and recover from disruptions in the future, GAO reviewed physical and electronic security measures, and BCP capabilities between February and June 2002 at 15 financial market organizations that perform trading and clearing functions, including 7 exchanges, 3 clearing and trade processing organizations, 3 electronic communications networks (ECN), and 2 payment system processors.² Stock and stock options exchanges match

¹Money markets instruments include federal funds, Treasury bills, commercial paper, and repurchase agreements.

²For simplicity, this report will refer to NASDAQ as an exchange.

orders from buyers and sellers to execute trades. Broker-dealers send these orders to the exchanges on behalf of individual investors or large institutional clients. Clearing organizations process trading information to ensure that buyers receive their securities and sellers receive their payments. ECNs provide alternative venues for trading securities. Payment system processors that transmit large dollar payments among banks are crucial to the basic functioning of the U.S. economy and financial markets. Banks also maintain accounts to pay for or receive payments from securities transactions for broker-dealers or their customers and, as custodians, maintain accounts for securities owned by their customers. For purposes of its analysis, GAO categorized 7 of the 15 organizations reviewed as more important than others on the basis of whether viable immediate substitutes existed for their products or services or whether the functions they performed were critical to the overall markets' ability to function.³ GAO relied on documentation and descriptions provided by market participants and regulators and reviews conducted by other organizations. When feasible, GAO also directly observed controls in place for physical security and business continuity at the organizations assessed. GAO did not test these controls by attempting to gain unauthorized entry or access to market participants' facilities or information systems. In assessing the organizations' physical and electronic security and BCPs, GAO used criteria that were generally accepted by government or industry, including that used to review federal organizations' information systems.⁴ GAO performed its work in various U.S. cities from November 2001 through October 2002.

Results in Brief

The financial markets were able to recover within days despite significant damage to the World Trade Center area, but the September 11, 2001, terrorist attacks also revealed that financial market participants would have to improve their business continuity capabilities. The attacks resulted

³For example, some exchanges transmit information on all executed trades or establish prices used by other exchanges. Also, clearing organizations or payment system processors are essential to overall market functioning because they often may be the only organizations that perform these functions.

⁴This guidance included the *Federal Information System Controls Audit Manual, Volume I: Financial Statement Audits* GAO/AIMD-12.19.6 (Washington, D.C.: Jan. 1999); the Federal Financial Institutions Examination Council's *FFIEC Information Systems Handbook: Volume 1*, (Washington, D.C.: 1996); and the Business Continuity Institute's *Business Guide to Continuity Management* (Worcester, United Kingdom: Jan. 19, 2001).

in significant loss of life and extensive physical damage, including to the telecommunications and power infrastructure, and physical access to the financial district was severely restricted for several days. Although the exchanges and clearing organizations largely escaped direct damage, trading did not resume on the stock and options markets because of damage to telecommunications, the lack of physical access to the affected area, and the loss of facilities and personnel by many broker-dealers, including firms representing 40 percent of normal market trading volume, and other financial institutions such as mutual funds and insurance companies that participated in these markets. Displaced firms and infrastructure providers made heroic efforts sometimes involving ad hoc and innovative solutions to recreate operations at new locations and restore needed telecommunications connections. Rather than trade without these significant firms and risk operational difficulties in the unstable conditions, regulators and market participants chose to conduct telecommunications testing over the weekend and the securities exchanges reopened on Monday, September 17, 2001, at record volumes. However, if any of the key exchanges or clearing organizations had been physically damaged, the markets would not have been able to open as quickly.

The markets for government securities and money market instruments were also significantly disrupted by the loss of key broker-dealer facilities and connectivity and processing difficulties that the Bank of New York, one of the two clearing banks for these markets, and its customers experienced. To prevent organizations from defaulting on their obligations and creating a widespread solvency crisis, the Federal Reserve provided over \$323 billion in funding to banks over the period from September 11 to September 14, 2001. Government securities trading resumed within 2 days but at much lower levels than normal and problems in settling some trades persisted for weeks. The impact of the attacks on the banking and payment systems was less severe because most banks' and payment processors' operations were located outside of the affected area.

Regulators and market participants have acknowledged that the attacks revealed the need to improve business continuity capabilities to address future disasters. At the time of the attacks, some market participants lacked backup facilities to which they could relocate their operations; others had backup facilities but they were located too close to their primary sites and were also inaccessible. Some organizations' backup sites were not large enough or did not have the equipment or software needed for critical operations. Many organizations also found that the arrangements they had made for backup telecommunications service were

inadequate. Financial institutions' plans had also called for their staff to assemble at designated locations or to proceed to their backup sites; but some organizations could not locate their staff, and some organizations' personnel had difficulty reaching alternative operating locations.

Although the 15 exchanges, clearing organizations, ECNs, and payment system processors that GAO reviewed had implemented various physical and information security measures and business continuity capabilities since the attacks, some organizations continued to have limitations in their preparations that increased the risk of their operations being disrupted by future disasters. Because hostile entities have openly threatened to directly attack participants in the U.S. financial markets in the future, the need for these organizations to be prepared has increased. However, reducing the risk of an operations disruption can require organizations to make trade-offs between implementing additional measures to protect their facilities and systems or using their resources to expand their business continuity capabilities. For example, an organization whose primary site is located in a highly trafficked, public area may have limited ability to reduce all of its physical security risks but could mitigate these risks by having a separately staffed backup facility or cross-training staff.

The 15 organizations GAO reviewed, including the 7 organizations whose ability to operate could be critical to the markets, have taken steps such as installing physical barriers around their facilities to prevent physical damage and using passwords or firewall software to limit access to information systems to prevent disruptions from electronic attacks. All 15 organizations had developed BCPs, including some that had established backup facilities hundreds of miles from their primary sites, that addressed procedures for restoring operations after a disaster. However, 9 of the 15 organizations, including 2 GAO considered critical to the functioning of the financial markets, had limitations in their protection and recovery measures, which increased the risk of their operations being disrupted. Although federal information systems standards and other guidance recommend having backup personnel, these 9 organizations had not developed business continuity procedures for ensuring that staff capable of conducting their critical operations would be available if an attack incapacitated personnel at their primary sites. At least 8 of the 9 organizations had physical vulnerabilities such as inability to control vehicular traffic around their facilities. Although most organizations had backup facilities as standards recommend, 10 of the 15 organizations, including 4 of the critical ones, faced increased risk of being unable to operate after a wide-scale disruption because they either lacked backup

facilities or had facilities within 2 to 10 miles of their primary site. Finally, although many of the 15 organizations had attempted to reduce their risks by testing their risk reduction measures, GAO found that few organizations had tested their physical security measures, and about half had tested their business continuity capabilities and key information systems protections.

Although banking and securities regulators have begun to take steps to prevent future disasters from causing widespread settlement and payment defaults, they have not taken important actions that would better ensure that trading in critical U.S. financial markets could resume in a fair and orderly way after a major disaster.⁵ The three regulators for major market participants, the Federal Reserve, the Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission (SEC) are working jointly with market participants to develop recovery goals and sound business continuity practices that will apply to a limited number of financial market organizations to ensure that these entities can clear and settle transactions and meet their financial obligations after future disasters. Although heroic efforts allowed the markets to recover after the September 11 attacks, future attacks could directly target critical financial market organizations and close the markets for an extended period. However, the regulators' recovery goals and sound practices would only apply to clearing activities and do not extend to organizations' trading activities or to the stock exchanges. Regulators told GAO that their efforts focus on clearing activities because clearing problems would pose the greatest risk to the markets and because one trading organization could replace another that was unable to operate in future disasters. However, without identifying specific recovery goals and sound business continuity practices for trading organizations, the appropriate exchanges, broker-dealers, and banks needed for trading to occur may not take all necessary steps to be operational. The regulators also had not developed complete strategies that identify where trading could be resumed or which organizations would have to be ready to conduct trading if a major exchange or multiple broker-dealers were unlikely to be operational for an extended period. SEC has proposed one strategy for resuming trading, but it does not include all securities, and it has not been fully tested.

⁵For additional discussion of how the financial markets are being addressed as part of U.S. efforts to protect critical infrastructure, see U.S. General Accounting Office, *Critical Infrastructure Protection: Efforts of Financial Services Sector to Address Cyber Threats*, GAO-03-173 (Washington D.C.: Jan. 30, 2003).

Individually, SEC, the Federal Reserve, and OCC have overseen operations risks in the past, but these efforts had not comprehensively addressed risks for all of the entities they regulate. Despite the importance of ensuring that the exchanges and clearing organizations are operational, SEC uses a voluntary program—the Automation Review Policy (ARP) program—to oversee how these organizations reduce risks to their operations. Under ARP, SEC staff have reviewed important risks at these institutions and spurred operations improvements. However, although SEC issued a rule requiring ECNs with sufficient trading volume to comply with the full range of ARP practices, they have not issued a similar rule to require the other 22 exchanges and clearing organizations subject to ARP to comply. However, GAO has found that some organizations, including critical organizations, have resisted developing recommended backup facilities or making other important improvements to address weaknesses SEC staff identified. Having a rule similar to that issued for the ECNs could provide SEC with flexible but specific regulatory authority to require all the organizations subject to ARP to take prudent actions when deemed necessary. The ARP program has had difficulties in maintaining experienced, qualified staff and lacks the resources to conduct examinations frequently. In addition, although the disruptions at key broker-dealers severely affected the markets' ability to resume trading after the attacks, the securities laws do not generally contain specific requirements applicable to such firms, and SEC's reviews therefore did not generally examine the extent to which broker-dealers had reduced their operations risks with regard to physical and information system security and BCP measures.

The Federal Reserve and OCC are tasked with overseeing the safety and soundness of banks' operations and had issued and were updating guidance that covered information system security and business continuity planning. Staff from these regulators told GAO that they conduct annual examinations of the largest entities they oversee and that they reviewed information security in all examinations and business continuity during most examinations, but the reviews did not generally assess banks' protections against terrorist attacks. GAO did not review bank examinations to independently determine the frequency and extensiveness of these regulators' reviews.

This report includes recommendations to SEC intended to ensure that the financial markets are better able to recover and resume operations in the event of a future disaster and to improve their individual oversight of operations risks. In commenting on a draft of this report, SEC agreed with the goals of our recommendations.

Principal Findings

September 2001 Attacks Significantly Affected U.S. Financial Markets and Demonstrated the Need for Improvements in BCPs

The September 2001 terrorist attacks and the subsequent collapse of the twin World Trade Center towers damaged more than 400 structures across a 16-acre area, and claimed almost 2,800 lives. Financial services industry employees accounted for about 74 percent of the victims. Dust and debris blanketed the area, creating difficult and hazardous conditions that complicated recovery efforts. Many financial organizations lost telecommunications service when the 7 World Trade Center building also collapsed and debris struck a major Verizon central switching office that served approximately 34,000 businesses and residences.⁶ Over 13,000 customers also lost power. To accommodate the rescue and recovery efforts and maintain order, pedestrian and vehicle access to the area encompassing the financial district was restricted through September 13, 2001.

As a result of the extensive damage to the area surrounding the World Trade Center and the need to ensure the health and safety of people affected by the attacks, U.S. financial markets closed on September 11 and took several days to resume operations. If the exchanges and clearing organizations had sustained direct damage, the reopening of the markets would have likely taken longer because some lacked backup operating facilities at the time. However, several key broker-dealers did sustain considerable damage and had to recreate their trading operations at other locations. These firms employed ad hoc and innovative solutions, such as renting out an entire hotel or moving their traders to the trading facilities of a recently purchased subsidiary. However, because these and other firms were unable to operate fully in the days following the attacks, securities regulators, market officials, and other key participants were concerned that insufficient liquidity would exist to conduct fair and orderly trading in the markets. By Friday, September 14, 2001, sufficient telecommunications capabilities to conduct trading had been restored to firms representing only about 60 percent of the normal order volume. After communications lines to the remaining firms were restored and tested, U.S. stock and options exchanges reopened on September 17, 2001, trading record volumes without noticeable difficulties. Full trading of U.S. government securities in

⁶Verizon is the major provider of local telecommunications service in lower Manhattan.

the United States was resumed within 2 days following the attacks but at lower-than-normal volumes, and funds transmittal problems at some institutions persisted for several days. The difficulties experienced by broker-dealers that trade government securities and the Bank of New York and its customers also disrupted the markets for short-term debt instruments that fund the operations of broker-dealers and other firms. To ensure that firms could meet their settlement obligations, the Federal Reserve had to provide over \$323 billion in liquidity to market participants by offering discount window loans, purchasing securities from participants needing funds, and taking other actions. Although some banks in Manhattan lost telecommunications service or experienced other disruptions, the U.S. banking system as a whole was not severely affected because most banks' facilities were located outside of the World Trade Center area. Similarly, the primary processors for most of the large-value payments between banks in the United States—Fedwire and the Clearing House Inter-bank Payments System—were also able to continue operating because their primary processing sites were located outside the affected area.

According to information GAO obtained from broker-dealers, banks, regulators, industry associations and others, the attacks revealed that improvements were needed in financial institutions' business continuity capabilities to address future disasters. Many financial institutions' BCPs addressed limited-scope events such as damage to just one of their buildings. As a result, many either had not established backup facilities or had backup facilities located near their primary facilities that were also destroyed or unusable. Others found that their backup facilities were too small and not properly equipped to accommodate all of their critical operations. In addition, some firms learned that the actions they had taken to ensure continuity of telecommunications service were not adequate. For example, after relocating their operations, some firms found that their backup facilities only had connections to the primary sites of organizations critical to their operations and not to the existing backup locations of other participants. Others whose facilities were not damaged also had to have telecommunications restored even though they thought that they had obtained redundant telecommunications capabilities by contracting with multiple telecommunications providers or by having their lines routed over different physical paths. In some cases, disruptions occurred because the alternative providers routed financial firms' lines through the same Verizon switching facility that was damaged by the attacks. Others whose services had originally used physically diverse paths found that their service providers had rerouted these lines over time onto identical pathways

without their knowledge. Recovery efforts at financial institutions were also hampered by shortcomings in the human capital component of BCPs. These firms had trouble locating critical personnel in the confusion after the attacks; and, in some cases, their staff had difficulty reaching backup locations as a result of the transportation shutdowns.

**Financial Market
Organizations Have Taken
Actions to Protect Facilities
and Information Systems
and Resume Operations
after Disruptions, but
Limitations Remain**

All 15 organizations that GAO reviewed, including the 7 critical organizations, had taken steps since the attacks to reduce the risk of operations disruptions by implementing measures to prevent physical damage to their facilities and unauthorized access to their information systems and developing business continuity capabilities to recover from disruptions.⁷ For example, many organizations had installed physical barriers to minimize damage or prevent unauthorized access by vehicles to their facilities. In addition, the 15 exchanges, clearing organizations, ECNs, and payment system processors used private networks and proprietary message formats that reduced the risk that they would be disrupted by electronic attacks. These organizations had also implemented various information security protections recommended for federal organizations, including hardware or software controls that allow only authorized users to gain system access and monitoring systems to detect attacks or intrusions. All 15 organizations also had developed BCPs addressing how they would continue operations after a disruption. For example, 11 of the 15 had established separate backup facilities, including 3 whose backup facilities were hundreds of miles away.

However, 9 of the 15 exchanges, clearing organizations, ECNs, and payment system processors, including 2 organizations critical to the functioning of the markets, had limitations in their risk reduction efforts. These 9 organizations were at greater risk of experiencing an operations disruption if a physical attack on their primary facility left a large percentage of their staff incapacitated because they did not maintain staff outside of their primary facility that could conduct all their critical operations. Eight of these 9 organizations also had physical security vulnerabilities at their primary sites that they either had not or could not mitigate, such as the inability to restrict vehicle movement around their facilities. In addition, 10 of the 15 organizations, including 4 critical organizations, had limitations in their BCPs that increased the risk of their

⁷This analysis presents the measures these organizations had in place at the time GAO conducted reviews at these entities' physical locations from February to June 2002.

operations being disrupted by a wide-scale disaster. These 10 organizations faced this risk because 4 lacked any backup facilities, and the backup facilities of the other 6 organizations were 2–10 miles from their primary sites—including 4 whose sites were separated by 5 miles or less. Another way that organizations can minimize their operations risk is by testing their physical and information security measures and BCPs, but GAO found that few of these organizations had fully tested all elements. Only 3 organizations had tested their physical security measures. Although all 7 of the critical organizations recently had assessed the vulnerabilities of their key trading and clearing systems, only 1 of the other 8 organizations had done so. Five of the critical organizations and 2 of the other 8 had tested their business continuity capabilities.

**Securities and Banking
Regulators Have Not
Developed Recovery Goals
for Resuming Trading
Activities and Their
Oversight of Operations
Risk Could Be Strengthened**

Securities and banking regulators have begun to jointly develop recovery goals and sound business continuity practices that will apply to market participants that perform clearing functions, but they have not identified recovery goals and practices for resuming trading activities. In August 2002, the Federal Reserve, OCC, SEC and the New York State Banking Department jointly issued a white paper seeking industry comment on sound practices to ensure that organizations that perform critical clearing activities be able to promptly recover these functions after a wide-scale, regional disruption.⁸ These sound practices could require organizations performing these functions to identify the clearing activities they perform to support critical markets, develop plans to recover clearing functions on the same business day, and maintain out-of-region recovery facilities that do not depend on the same labor pool or transportation, telecommunications, water, and power infrastructure. The practices would be applied to clearing organizations, clearing banks, and to the clearing functions of about 15 to 20 active broker-dealers and banks whose transaction volumes, if not promptly cleared and settled, could create liquidity or solvency problems for organizations awaiting payments from them. The regulators are still analyzing the comments that they have received but hoped to issue a final version of the practices in 2003. GAO agrees that taking actions to ensure that clearing functions can be recovered after a disaster is important to the U.S. financial markets and the

⁸Board of Governors of the Federal Reserve, OCC, SEC, *Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, (Washington, D.C.: Aug. 30, 2002). The New York State Banking Department issued the same paper separately.

economy overall, and that sound business continuity practices, if adopted, would likely reduce the potential for future disasters to cause broader financial crises.

However, trading on U.S. financial markets is also a critical economic function for investing savings, funding daily business operations, and raising capital for new ventures; but the securities regulators have not similarly begun efforts to develop recovery goals and business continuity practices applicable to trading activities in stock, options, and other financial markets. Regulatory staff told GAO that the white paper's practices apply only to clearing activities because such functions are usually concentrated in single entities for some markets or in very few organizations for others, and thus pose a greater potential for disruption. They said the paper does not cover trading activities and organizations that conduct only trading, such as the securities exchanges, because other organizations could perform the same functions. Although trading could likely be moved to other venues if a major exchange was not able to operate after a disaster, such transfers have not been frequently done and could be subject to operational problems such as insufficient processing capacity if not clearly established and tested in advance. Securities regulators have not developed complete strategies for ensuring that trading could resume when appropriate. For example, SEC has asked two major exchanges—New York Stock Exchange and the NASDAQ, which each trade thousands of securities—to be able to trade each other's securities as one strategy for ensuring that trading could resume if either organization was unable to operate. However, as of December 2002, SEC had not identified the specific capabilities that these organizations should implement. For example, NASDAQ staff said that various alternatives are being proposed for conducting this trading and each would involve varying amounts of system changes or processing capacity considerations. New York Stock Exchange staff said they have proposed trading only the top 250 of NASDAQ's securities, and the others would have to be traded elsewhere. NASDAQ staff plan to trade all New York Stock Exchange securities. These strategies have also not been fully tested to ensure that processing can occur accurately and that each exchange has sufficient capacity.

Although the attacks demonstrated sufficient numbers of broker-dealers have to be able to recover their trading operations and provide access to their customers' cash and securities for markets to resume operating smoothly and in a timely manner, the regulators have not similarly developed recovery goals and sound business continuity practices applicable to these firms' trading or brokerage activities. With hostile

entities openly targeting U.S. financial markets, setting recovery goals and ensuring that the appropriate organizations have adopted sound business continuity practices would reduce the risk that trading may not be able to resume smoothly or in a timely manner if key market participants are severely damaged.

Regulators' Oversight of Operations Risks Had Limitations

Although SEC has reviewed operations risk at exchanges and clearing organizations, its oversight has limitations. In response to operational problems experienced by the markets during the 1980s, SEC created a program in 1989 for addressing operations risk issues, including physical and information security and business continuity planning at securities exchanges and clearing organizations. SEC did not create rules for these organizations to follow but instead issued two ARP statements that provided practices in various information technology and operational areas with which the exchanges and clearing organizations would be expected to comply voluntarily. By analyzing all 10 of the SEC ARP examination reports completed between January 2001 and July 2002, GAO found that SEC ARP staff had reviewed information security in 9 of these examinations and business continuity in 7. SEC ARP staff reviewed physical security and controls at data centers, but they discussed organizations' overall physical security in only one report. Although none of the 10 reports GAO reviewed discussed how these organizations' BCPs covered telecommunications resiliency, ARP staff said that all of these operations risk issues would be addressed as part of future reviews.

Given the increased threats demonstrated by the September 11 attacks and the need for assurance that key financial market organizations are following sound practices, the importance of SEC's ARP program oversight has increased. However, currently the program faces several limitations. Although the efforts of SEC's ARP staff have improved market participant operations, only ECNs are required by rule to comply with ARP policies and exchanges and clearing organizations are expected to comply voluntarily. Although SEC staff said they have been satisfied with the level of these organizations' compliance, GAO reported in 2001 that some organizations, including critical organizations, had not taken actions to address important weaknesses ARP staff identified. For example, SEC had long-standing concerns that three exchanges lacked backup facilities and that another major exchange had insufficient processing capacity for

several years.⁹ GAO analysis of recent ARP reviews indicated that SEC staff continue to identify significant weaknesses at some organizations. Having a rule that requires these organizations to engage in practices consistent with the ARP policies would provide SEC staff with the flexibility to adjust ARP expectations as technology and industry best practices evolve while providing specific regulatory authority to require prudent actions when deemed necessary. The ARP program has also faced resource limitations. During work conducted as part of a prior GAO review of overall SEC operations, market participants raised concerns over the inexperience and insufficient technical expertise of ARP staff that reviewed their organizations.¹⁰ In addition, SEC staff said that the staffing level limits their ability to conduct more frequent reviews of the organizations subject to ARP. GAO's analysis of the frequency of ARP examinations found that an average of 39 months had passed between the most recent and prior examinations for the organizations critical to the markets that are subject to ARP. In contrast, guidance for audits of federal information systems calls for high-risk systems to be reviewed more frequently.

Operations Risks Not Generally Reviewed at Broker-Dealers

Lacking specific requirements in the securities laws or SRO rules, SEC and exchange reviews of broker-dealers have also not generally addressed operational issues such as physical and information security and BCPs. Whereas SEC ARP staff review exchanges and clearing organizations, staff from SEC's Office of Compliance Inspections and Examinations (OCIE) conduct examinations of broker-dealers, mutual funds, and other securities market participants.¹¹ Prior to the September 11 attacks, OCIE staff only reviewed operational issues at a few broker-dealers that offered on-line trading. The exchanges, which act as self-regulatory organizations and conduct their own reviews of their members, and SEC OCIE staff also have recently begun conducting reviews relating to information security issues as the result of Gramm-Leach-Bliley Act, which requires financial institutions to safeguard customer information. The SROs also plan to review their broker-dealer members' compliance with rules recently

⁹GAO reported on these issues in 2001. See U.S. General Accounting Office, *Information Systems: Opportunities Exist to Strengthen SEC's Oversight of Capacity and Security*, GAO-01-863 (Washington, D.C.: Jul. 25, 2001).

¹⁰See U.S. General Accounting Office, *SEC Operations: Increased Workload Creates Challenges*, GAO-02-302 (Washington, D.C.: Mar. 5, 2002).

¹¹Other market participants that SEC oversees include investment advisers and transfer agents.

submitted for SEC approval, which will require these firms to develop BCPs.

Bank Regulators Report
Overseeing Operations Risks but
Not Banks' Measures Against
Physical Attacks

Because the banking regulators are required to assess the safety and soundness of bank operations, in 1996, the banking regulators jointly developed guidance for their staff and the institutions they oversee relating to information security and business continuity issues. They intend to issue more expanded guidance on information security and business continuity in early 2003. The banking regulators also conduct examinations that address operational issues as part of their regular cycle of annual reviews. Staff from the Federal Reserve and OCC, which oversee the majority of the largest institutions, indicated that they examine information security at all banks and business continuity during most examinations. They also said that their examiners or bank internal auditors review banks' physical security, but these reviews were not generally focused on the extent to which institutions have protected themselves from terrorist or other physical attacks. GAO did not review bank examinations to independently determine the frequency and extensiveness of these regulators reviews.

Recommendations

This report includes recommendations to the Chairman, SEC, to work with industry to develop goals and strategies to resume trading in securities markets; determine sound business continuity practices that organizations would need to follow to meet these goals; identify the organizations, including broker-dealers, that would likely need to operate for the markets to resume trading and ensure that these organizations implement sound business continuity practices that, at a minimum, allow investors to readily access their cash and securities; and test trading resumption strategies to better ensure their success. The report also recommends that SEC improve its oversight of operations risk by issuing a rule to require exchanges and clearing organizations to engage in practices consistent with its ARP program and expand the resources dedicated to the ARP program.

Agency Comments and GAO Evaluation

GAO requested comments on a draft of this report from the heads, or their designees, of the Federal Reserve, OCC, Treasury, and SEC. The Federal Reserve and SEC provided written comments, which appear in appendixes III and IV, respectively. The Federal Reserve, OCC, and SEC also provided technical comments, which were incorporated as appropriate. SEC generally agreed with the report and the goals of its recommendations. The SEC staff's letter agreed that the financial markets should be prepared to

resume trading in a timely, fair, and orderly fashion following a catastrophe, which is the goal of GAO's recommendations that SEC work with the industry to develop business continuity goals, strategies, and practices. SEC's letter expressed a concern that this recommendation expects SEC to ensure that broker-dealers implement business continuity practices that would allow trading activities to resume after a disaster. The SEC staff noted that, although broker-dealers are required to be able to ensure that any completed trades are cleared and settled and that customers have access to the funds and securities in their accounts as soon as is physically possible, these firms are not required to conduct trading or provide liquidity to markets. Instead, this is a business decision on the part of these firms' management. As a result, SEC's letter stated that the BCP expectations for these firms must reflect these considerations.

GAO agreed that the business continuity practices that SEC develops in conjunction with market participants should reflect these considerations. As SEC works with the exchanges and other market participants to develop goals and strategies for recovering from various disaster scenarios, GAO's recommendations envision that these strategies will have to take into account the business continuity capabilities implemented by broker-dealers that normally provide significant order flow and liquidity to the markets. To the extent that many of these major broker-dealers may be unable to conduct their normal volume trading in the event of some potential disasters without extended delays, SEC would need to develop strategies that would allow U.S. securities markets to resume trading when appropriate through other broker-dealers that are less affected by the disaster, such as regional firms. To ensure that such trading is orderly and fair to all investors, broker-dealers' business continuity practices should at least be adequate to allow prompt transfers of customer funds and securities to other firms so that the customers of firms unable to resume trading are not disadvantaged. In response to GAO's recommendations relating to ARP, the SEC staff's letter states that they will continue to assess whether rulemaking is appropriate and will consider recommending to the Chairman that ARP staffing and resources be expanded if the agency's funding is increased.

Introduction

Thousands of market participants are involved in trading stocks, options, government bonds, and other financial products in the United States. These participants include exchanges at which orders to buy and sell are executed, broker-dealers who present those orders on behalf of their customers, clearing organizations that ensure that ownership is transferred, and banks that process payments for securities transactions. Although many organizations are active in the financial markets, some organizations, such as the major exchanges, clearing firms, and large broker-dealers are more important for the overall market's ability to function because they offer unique products or perform vital services. The participants in these markets are overseen by various federal securities and banking regulators whose regulatory missions vary. Financial markets also rely heavily on information technology systems and extensive and sophisticated communications networks. As a result, physical and electronic security measures and business continuity planning are critical to maintaining and restoring operations in the event of a disaster or attack.

Various Organizations Participate in Stock and Options Markets

Customer orders for stocks and options, including those from individual investors and from institutions such as mutual funds, are usually executed at one of the many exchanges located around the United States.¹ Currently, stocks are traded on at least eight exchanges, including the New York Stock Exchange (NYSE), the American Stock Exchange, and the NASDAQ.² Securities options are traded at five exchanges, including the Chicago Board Options Exchange and the Pacific Stock Exchange. Trading on the stock exchanges usually begins when customers' orders are routed to the exchange floor either by telephone or through electronic systems to specialist brokers. These brokers facilitate trading in specific stocks by matching orders to buy and sell. For stocks traded on NASDAQ, customers' orders are routed for execution to the various brokers who act as market makers by posting price quotes at which they are willing to buy or sell particular securities on that market's electronic quotation system. Some stocks traded on NASDAQ can be quoted by just a single broker making a market for that security, but others have hundreds of brokers acting as

¹Securities options are contracts that provide the right for the purchaser to buy or sell a specified quantity of a security at a specified price at a future date.

²Although currently operating as a market operated by an association of dealers, NASDAQ is seeking to become registered with SEC as a national securities exchange, and for simplicity, we will refer to it as an exchange in this report.


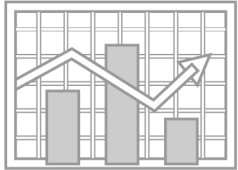
market makers in a particular security by buying and selling shares from their own inventories. Orders for options are often executed on the floors of an exchange in an open-outcry pit in which the representatives of sometimes hundreds of brokers buy and sell options contracts on behalf of their customers.

The orders executed on the various markets usually come from broker-dealers. Individual and institutional investors open accounts with these firms and, for a per-transaction commission or an annual fee, the broker-dealer buys and sells stocks, bonds, options, and other securities on the customers' behalf. Employees of these firms may provide specific investment advice or develop investment plans for investors. Although some firms only offer brokerage services and route customer orders to other firms or exchanges for execution, some also act as dealers and fill customer orders to buy or sell shares from their own inventory.

In addition to the exchanges, customers' orders can also be executed on electronic communications networks (ECN), which match their customers' buy and sell orders to those submitted by their other customers. The various ECNs specialize in providing different services to their customers such as rapid executions or anonymous trading for large orders.

After a securities trade is executed, the ownership of the security must be transferred and payment must be exchanged between the buyer and the seller. This process is known as clearance and settlement. Figure 1 illustrates the clearance and settlement process and the various participants, including broker-dealers, the clearing organization for stocks (the National Securities Clearing Corporation or NSCC), and the Depository Trust Company (which maintains records of ownership for the bulk of the securities traded in the United States).

Figure 1: Clearance and Settlement Process for Stocks

Day 1 (T)	Day 2 (T+1)	Day 3 (T+2)	Day 4 (T+3)
<ul style="list-style-type: none"> - Trade is executed on exchange - Trade details (price and number of shares) provided to buying and selling broker-dealers for comparison 	<ul style="list-style-type: none"> - Trade comparison completed - NSCC assumes the obligations of the broker-dealers on either side of a trade to guarantee that buyers will receive their shares and that sellers will get paid 	<ul style="list-style-type: none"> - NSCC nets all buy and sell obligations of each broker-dealer together and provides reports to these firms as to whether they were net sellers or net buyers of a particular security - NSCC notifies broker-dealers whose selling activity exceeds their securities purchases to expect a payment to be sent to their clearing bank - NSCC notifies broker-dealers whose buying activity exceeds their securities sales to remit funds to NSCC's bank 	<ul style="list-style-type: none"> - Funds are exchanged between the broker-dealers' and NSCC's banks - Ownership of shares is transferred from selling broker-dealers to those firms that made purchases in the accounts maintained for these firms by the Depository Trust Company - Broker-dealers add shares purchased and remove shares sold from the records of customer accounts

Source: GAO analysis of NSCC data.

The Options Clearing Corporation plays a similar role in clearing and settling securities options transactions. After options trades are executed, the broker-dealers on either side of the trade compare trade details with each other, and the clearing organization and payments are exchanged on T+1.

Banks also participate in U.S. securities markets in various ways. Some banks act as clearing banks by maintaining accounts for broker-dealers and accepting and making payments for these firms. Some banks also act as custodians of securities by maintaining custody of securities owned by other financial institutions or individuals.

Government Securities and Money Market Instruments Are Traded Differently from Stocks

The market for the U.S. government securities issued by the Department of the Treasury (Treasury) is one of the largest markets in the world. These securities include Treasury bills, notes, and bonds of varying maturities. Trading in government securities does not take place on organized exchanges. Instead, these securities are traded in an “over-the-counter” market and are carried out by telephone calls between buying and selling dealers. To facilitate this trading, a small number of specialized firms, known as inter-dealer brokers (IDB) act as intermediaries and arrange trades in Treasury securities between other broker-dealers. The use of the IDBs allows other broker-dealers to maintain anonymity in their trading

activity, which reduces the likelihood that they will obtain disadvantageous prices when buying or selling large amounts of securities.

Trades between the IDBs and other broker-dealers are submitted for clearance and settled at the Government Securities Clearing Corporation (GSCC). After trade details are compared on the night of the trade date, GSCC provides settlement instructions to the broker-dealers and their clearing banks. Settlement with these banks and the clearing organization's bank typically occurs one business day after the trade (T+1) with ownership of securities bought and sold transferred either on the books of clearing banks or the books of the Federal Reserve through its Fedwire Securities Transfer System. Two banks, JPMorgan Chase and the Bank of New York, provide clearing and settlement services for many major broker-dealers in the government securities market.

Many of the same participants in the government securities markets are also active in the markets for money market instruments. These are short-term instruments that include federal funds,³ foreign exchange transactions, and commercial paper. Commercial paper issuances are debt obligations issued by banks, corporations, and other borrowers to obtain financing for 1 to 270 days. Another type of money market instrument widely used for short-term financing is the repurchase agreement or repo, in which a party seeking financing sells securities, typically government securities, to another party while simultaneously agreeing to buy them back at a future date, such as overnight or some other set term. The seller obtains the use of the funds exchanged for the securities, and the buyer earns a return on their funds when the securities are repurchased at a higher price than originally sold. Active participants in the repo market include the Federal Reserve, which uses repos in the conduct of monetary policy, and large holders of government securities, such as foreign central banks or pension funds, which use repos to obtain additional investment income. Broker-dealers are active users of repos for financing their daily operations. To facilitate this market, the IDBs often match buyers and sellers of repos; and the funds involved are exchanged between the government securities clearing organization and the clearing banks of market participants. According to data reported by the Federal Reserve, repo transactions valued at over \$1 trillion occur daily in the United States.

³Federal funds are balances deposited by commercial banks at Federal Reserve Banks to meet reserve requirements. These amounts can be lent among banks.

Payment Systems Processors Transfer Funds for Financial Markets and Other Transactions

Payments for corporate and government securities transactions, as well as for business and consumer transactions, are transferred by payment system processors. One of these processors is the Federal Reserve, which owns and operates the Fedwire Funds Transfer System. Fedwire connects 9,500 depository institutions and electronically transfers large dollar value payments associated with financial market and other commercial activities in the United States. Fedwire is generally the system used to transfer payments for securities between the banks used by the clearing organization and market participants. Another large dollar transfer system is the Clearing House Inter-bank Payments System (CHIPS). CHIPS is a system for payment transfers, particularly for those U.S. dollar payments relating to foreign exchange and other transactions between banks in the United States and in other countries.

Certain Market Participants Are Critical to Overall Functioning of the Securities Markets

Although thousands of entities are active in the U.S. securities markets, certain key participants are critical to the ability of the markets to function. Although multiple markets exist for trading stocks or stock options, some are more important than others as a result of the products they offer or the functions they perform. For example, an exchange that attracts the greatest trading volume may act as a price setter for the securities it offers, and the prices for trades that occur on that exchange are then used as the basis for trades in other markets that offer those same securities. On June 8, 2001, when a software malfunction halted trading on NYSE, the regional exchanges also suspended trading although their systems were not affected. Other market participants are critical to overall market functioning because they consolidate and distribute price quotations or information on executed trades. Markets also cannot function without the activities performed by the clearing organizations; and in some cases, only one clearing organization exists for particular products.

In contrast, disruptions at other participants may have less severe impacts on the ability of the markets to function. For example, many of the options traded on the Chicago Board Options Exchange are also traded on other U.S. options markets. Thus if this exchange was not operational, investors would still be able to trade these options on the other markets, although certain proprietary products, such as options on selected indexes, might be unavailable temporarily.

Other participants may be critical to the overall functioning of the markets only in the aggregate. Investors can choose to use any one of thousands of

broker-dealers registered in the United States. If one of these firms is unable to operate, its customers may be inconvenienced or unable to trade, but the impact on the markets as a whole may just be a lower level of liquidity or reduced price competitiveness. But a small number of large broker-dealers account for sizeable portions of the daily trading volume on many exchanges and if several of these large firms are unable to operate, the markets might not have sufficient trading volume to function in an orderly or fair way.

Various Regulators Oversee Securities Market Participants, but Approaches and Regulatory Goals Vary

Several federal organizations oversee the various securities market participants. The Securities and Exchange Commission (SEC) regulates the stock and options exchanges and the clearing organizations for those products. In addition, SEC regulates the broker-dealers that trade on these markets and other participants, such as mutual funds, which are active investors. The exchanges also have responsibilities as self-regulatory organizations (SRO) for ensuring that their participants comply with the securities laws and the exchanges' own rules.

SEC or one of the depository institution regulators oversees participants in the government securities market, but Treasury also plays a role. Treasury issues rules pertaining to that market, but SEC or the bank regulators are responsible for conducting examinations to ensure that these rules are followed.

Several federal organizations have regulatory responsibilities over banks and other depository institutions, including those active in the securities markets. The Federal Reserve oversees bank holding companies and state-chartered banks that are members of the Federal Reserve System. The Office of the Comptroller of the Currency (OCC) examines nationally chartered banks.⁴

Securities and banking regulators have different regulatory missions and focus on different aspects of the operations of the entities they oversee. Because banks accept customer deposits and use those funds to lend to borrowers, banking regulators focus on the financial soundness of these institutions to reduce the likelihood that customers will lose their deposits.

⁴Other organizations that oversee depository institutions include the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration.

Poor economic conditions or bank mismanagement have periodically led to extensive bank failures and customer losses in the United States. As a result, banking and the other depository institution regulators issue guidance and conduct examinations over a wide range of financial and operational issues pertaining to these institutions, such as what information security steps these institutions have taken to minimize unauthorized access to their systems and what business continuity capabilities they have.

In contrast, securities regulators have a different mission and focus on other aspects of the operations of the entities they oversee. Securities regulation in the United States arose with the goal of protecting investors from abusive practices and ensuring that they were treated fairly. To achieve this, SEC and the exchanges, which act as self regulatory organizations (SRO) to oversee their broker-dealer members, focus primarily on monitoring securities market participants to ensure that the securities laws are not being violated; for example, restricting insider trading or requiring companies issuing securities to completely and accurately disclose their financial condition. As a result, few securities regulations specifically address exchange and broker-dealer operational issues, and securities regulators have largely considered the conduct of such operations to be left to the business decisions of these organizations.

Telecommunications and Information Technology Are Vital to Securities Markets

Information technology and telecommunications are vital to the securities markets and the banking system. Exchanges and markets rely on information systems to match orders to buy and sell securities for millions of trades. They also use such systems to instantaneously report trade details to market participants in the United States and around the world. Information systems also compile and compare trading activity and determine all participants' settlement obligations. The information exchanged by these information systems is transmitted over various types of telecommunications technology, including fiber optic cable.

Broker-dealers also make extensive use of information technology and communications systems. These firms connect not only to the networks of the exchanges and clearing organizations but may also be connected to the thousands of information systems or communications networks operated by their customers, other broker-dealers, banks, and market data vendors. Despite widespread use of information technology to transmit data, securities market participants are also heavily dependent on voice communications. Broker-dealers still use telephones to receive, place, and

confirm orders. Voice or data lines transmit the information for the system that provides instructions for personnel on exchange floors. Fedwire and CHIPS also rely heavily on information technology and communications networks to process payments. Fedwire's larger bank customers have permanent network connections to computers at each of Fedwire's data centers, but smaller banks connect via dial-up modem. CHIPS uses fiber-optic networks and mainframe computers to transfer funds among its 54 member banks.

Financial Organizations Manage Operations Risks by Protecting Physical and Information Security and Business Continuity Planning

Because financial market participants' operations could be disrupted by damage to their facilities, systems, or networks, they often invest in physical and information security protection and develop business continuity capabilities to ensure they can recover from such damage. To reduce the risk that facilities and personnel would be harmed by individuals or groups attempting unauthorized entry, sabotage, or other criminal acts, market participants invest in physical security measures such as guards or video monitoring systems. Market participants also invest in information security measures such as firewalls, which reduce the risk of damage from threats such as hackers or computer viruses. Finally, participants invest in business continuity capabilities, such as backup locations, that can further reduce the risk that damage to primary facilities will disrupt an organization's ability to continue operating.

Objectives, Scope, and Methodology

To describe the impact of the September 11, 2001, attacks on the financial markets and the extent to which organizations had been prepared for such events, we reviewed studies of the attacks' impact by regulators and private organizations. We also obtained documents and interviewed staff from over 30 exchanges, clearing organizations, broker-dealers, banks, and payment system processors, including organizations located in the vicinity of the attacks and elsewhere. We toured damaged facilities and discussed the attacks' impact on telecommunications and power infrastructure with three telecommunications providers (Verizon, AT&T, and WorldCom) and Con Edison, a power provider. Finally, we discussed the actions taken to stabilize the markets and facilitate their reopening with financial market regulators.

To determine how financial market organizations were attempting to reduce the risk that their operations could be disrupted, we selected 15 major financial market organizations that included many of the most active

participants, including 7 stock and options exchanges, 3 clearing and securities processing organizations, 3 ECNs, and 2 payment system processors. For purposes of our analysis, we also categorized these organizations into two groups: seven whose ability to operate is critical to the overall functioning of the financial markets and eight for whom disruptions in their operations would have a less severe impact on the overall markets. We made these categorizations by determining whether viable immediate substitutes existed for the products or services the organizations offer or whether the functions they perform were critical to the overall markets' ability to function. To maintain the organizations' security and the confidentiality of proprietary information, we agreed with these organizations that we would not discuss how they were affected by the attacks or how they were addressing their risks through physical and information security and business continuity efforts in a way that could identify them. However, to the extent that information about these organizations is already publicly known, we sometimes name them in the report.

To determine what steps these 15 organizations were taking to reduce the risks to their operations from physical attacks, we conducted on-site "walkthroughs" of these organizations' primary facilities, reviewed their security policies and procedures, and met with key officials responsible for physical security to discuss these policies and procedures. We compared these policies and procedures to 52 standards developed by the Department of Justice for federal buildings.⁵ Based on these standards, we evaluated these organizations' physical security efforts across several key operational elements, including measures taken to secure perimeters, entryways, and interior areas and whether organizations had conducted various security planning activities.

To determine what steps these 15 organizations were taking to reduce the risks to their operations from electronic attacks, we reviewed the security policies of the organizations we visited and reviewed documentation of their system and network architectures and configurations. We also

⁵See Department of Justice, *Vulnerability Assessment of Federal Facilities*, (Washington, D.C.: June 28, 1995), which presents security standards that were developed following the bombing of the Murrah Building in Oklahoma City in 1995 and are intended to be used to assess security at all federal facilities. Under the standards, each facility is to be placed in five categories, with Level 1 facilities having the least need for physical security and Level 5 facilities having the highest need. Based on its risk level, a facility would be expected to implement increasingly stringent measures in 52 security areas.

compared their information security measures to those recommended for federal organizations in the Federal Information System Controls Audit Manual (FISCAM).⁶ Using these standards, we attempted to determine through discussions and document reviews how these organizations had addressed various key operational elements for information security, including how they controlled access to their systems and detected intrusions, what responses they made when such intrusions occurred, and what assessments of their systems' vulnerabilities they had performed.

To determine what steps these 15 organizations had taken to ensure they could resume operations after an attack or other disaster, we discussed their business continuity plans (BCP) with staff and toured their primary facilities and the backup facilities they maintained.⁷ In addition, we reviewed their BCPs and assessed them against practices recommended for federal and private-sector organizations, including FISCAM, bank regulatory guidance, and the practices recommended by the Business Continuity Institute.⁸ Comparing these standards with the weaknesses revealed in some financial market participants' recovery efforts after the September 2001 attacks, we determined how these organizations' BCPs addressed several key operational elements. Among the operational elements we considered were the existence and capabilities of backup facilities, whether the organizations had procedures to ensure the availability of critical personnel and telecommunications, and whether they completely tested their plans. In evaluating these organizations' backup facilities, we attempted to determine whether these organizations had backup facilities that would allow them to recover from damage to their primary sites or from damage or inaccessibility resulting from a wide-scale disaster. We also met with staff of several major banks and securities firms to discuss their efforts to improve BCPs. We also reviewed results of a survey by the NASD—which oversees broker-dealer members of

⁶U.S. General Accounting Office, *Federal Information Systems Controls Audit Manual, Volume I: Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: Jan. 1999).

⁷We conduct our reviews of these 15 organizations physical and electronic security measures and BCP capabilities between February and June 2002. When feasible, we also directly observed controls in place for physical security and business continuity at the organizations assessed. We did not test these controls by attempting to gain unauthorized entry or access to market participants' facilities or information systems.

⁸This guidance included FISCAM; the Federal Financial Institutions Examination Council's *Information Systems Handbook: Volume 1* (Washington, D.C.: 1996); and the Business Continuity Institute's *Business Guide to Continuity Management* (Worcester, United Kingdom: Jan. 19, 2001).

NASDAQ—that reported on the business continuity capabilities of 120 of its largest members and a random selection of 150 of approximately 4,000 remaining members.

To assess how the financial regulators were addressing physical security, electronic security, and business continuity planning at the financial institutions they oversee, we met with staff from SEC, the Federal Reserve, OCC, and representatives of the Federal Financial Institutions Examination Council. In addition, we met with NYSE and NASD staff responsible for overseeing their members' compliance with the securities laws. At SEC, we also collected data on the examinations SEC had conducted of exchanges, clearing organizations, and ECNs since 1995 and reviewed the examiners' work program and examination reports for the 10 examinations completed between July 2000 and August 2002. In addition, we reviewed selected SEC and NYSE examinations of broker-dealers.

To determine how the financial markets were being addressed as part of the United States' critical infrastructure protection efforts, we reviewed previously completed GAO work, met with staff from Treasury and representatives of the Financial and Banking Information Infrastructure Committee (FBIIC), which is undertaking efforts to ensure that critical assets in the financial sector are protected. We also discussed initiatives to improve responses to future crises and improve the resiliency of the financial sector and its critical telecommunications services with representatives of industry trade groups, including the Bond Market Association and the Securities Industry Association, as well as regulators, federal telecommunications officials, telecommunications providers, and financial market participants. The results of this work are presented in appendix II.

We conducted our work in various U.S. cities from November 2001 to October 2002 in accordance with generally accepted government auditing standards.

September 11 Attacks Severely Disrupted U.S. Financial Markets

The terrorist attacks on September 11, 2001, resulted in significant loss of life and extensive property and other physical damage, including damage to the telecommunications and power infrastructure serving lower Manhattan. Because many financial market participants were concentrated in the area surrounding the World Trade Center, U.S. financial markets were severely disrupted. Several key broker-dealers experienced extensive damage, and the stock and options markets were closed for the longest period since the 1930s. The markets for government securities and money market instruments were also severely disrupted as several key participants in these markets were directly affected by the attacks. However, financial market participants, infrastructure providers, and regulators made tremendous efforts to successfully reopen these markets within days. Regulators also took various actions to facilitate the reopening of the markets, including granting temporary relief from regulatory reporting and other requirements and providing funds and issuing securities to ensure that financial institutions could fund their operations. The impact on the banking and payments systems was less severe, as the primary operations of most banks and payment systems processors were located outside of the area affected by the attacks, or because they had fully operational backup facilities in other locations. Although many factors affected the ability of the markets to resume operations, the attacks also revealed limitations in many participants' BCPs for addressing such a widespread disaster. These factors included not having backup facilities that were sufficiently geographically dispersed or comprehensive enough to conduct all critical operations, unanticipated loss of telecommunications service, and difficulties in locating staff and transporting them to new facilities.

Attacks Caused Extensive Damage and Loss of Life and Created Difficult Conditions That Impeded Recovery Efforts

On September 11, 2001, two commercial jet airplanes were hijacked by terrorists and flown into the twin towers of the World Trade Center. Within hours, the two towers completely collapsed, resulting in the loss of four other buildings that were part of the World Trade Center complex. As shown in figure 2, the attacks damaged numerous structures in lower Manhattan.

Figure 2: Buildings Destroyed or Damaged on September 11, 2001



Source: Urban Data Solutions Inc.

The attacks caused extensive property damage. According to estimates by the Securities Industry Association, the total cost of the property damages ranges from \$24 to \$28 billion. According to one estimate, the damage to structures beyond the immediate World Trade Center area extended across 16 acres. The six World Trade Center buildings that were lost accounted for

over 13 million square feet of office space, valued at \$5.2 to \$6.7 billion.¹ One of these buildings was 7 World Trade Center, which was a 46-story office building directly to the west of the two towers. It sustained damage as a result of the attacks, burned for several hours, and collapsed around 5:00 p.m. on September 11, 2001. An additional nine buildings containing about 15 million square feet of office space were substantially damaged and were expected to require extensive and lengthy repair before they could be reoccupied. Sixteen buildings with about 10 million square feet of office space sustained relatively minor damage and will likely be completely reoccupied. Finally, another 400 buildings sustained damage primarily to facades and windows. A study by an insurance industry group estimated that the total claims for property, life, and other insurance would exceed \$40 billion.² In comparison, Hurricane Andrew of 1992 caused an estimated \$15.5 billion in similar insurance claims.

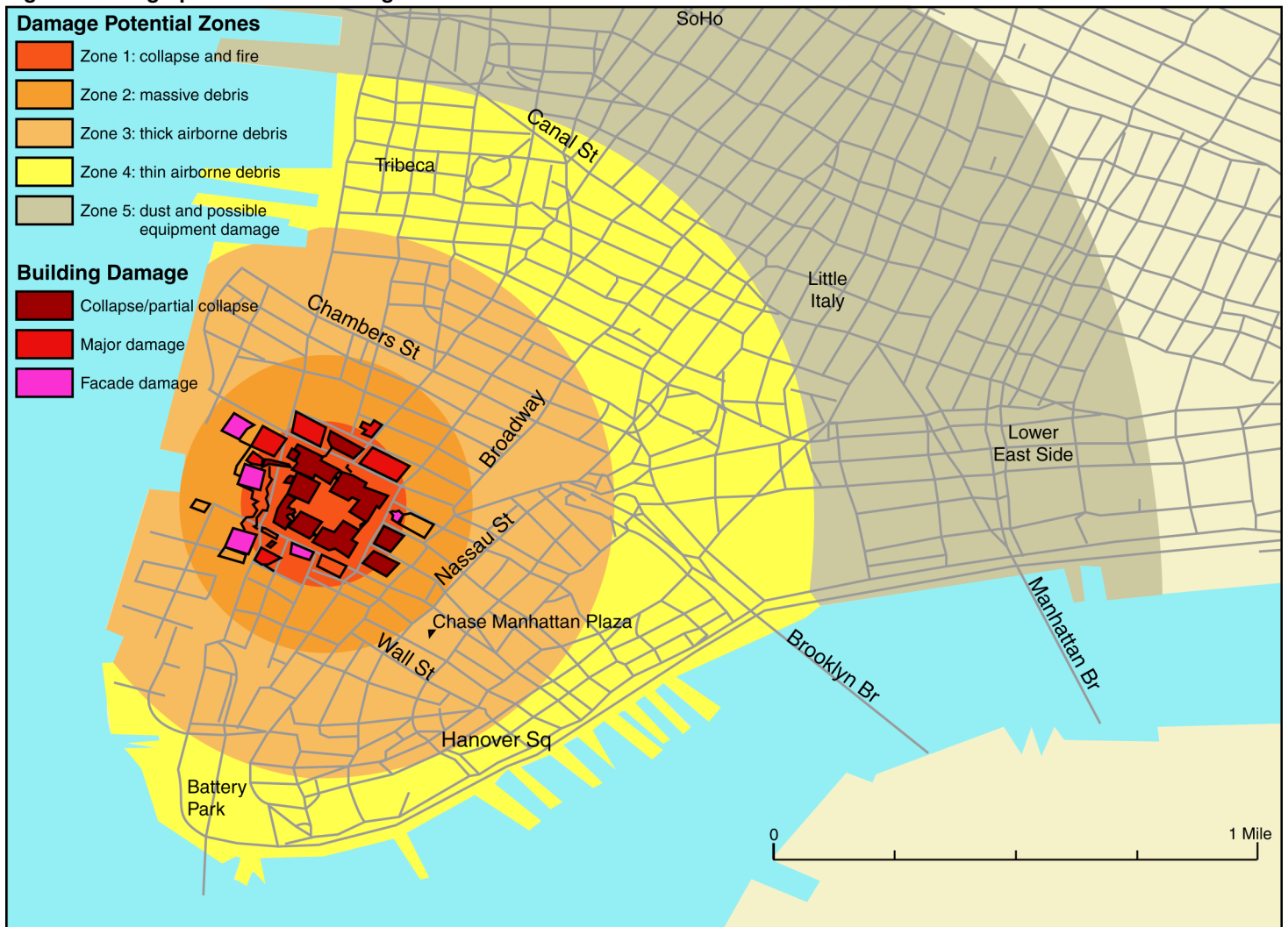
The loss of life following the attacks on the World Trade Center was also devastating with the official death toll for the September 11 attacks reaching 2,795, as of November 2002. Because of the concentration of financial market participants in the vicinity of the World Trade Center, a large percentage of those killed were financial firm employees. Excluding the 366 members of the police and fire departments and the persons on the airplanes, the financial industry's loss represented over 74 percent of the total civilian casualties in the World Trade Center attacks. Four firms accounted for about a third of the civilian casualties, and 658 were employees of one firm—Cantor Fitzgerald, a key participant in the government securities markets. The loss of life also exacted a heavy psychological toll on staff that worked in the area, who both witnessed the tragedy and lost friends or family. Representatives of several organizations we met with told us that one of the difficulties in the aftermath of the attacks was addressing the psychological impact of the event on staff. As a result, individuals attempting to restore operations often had to do so under emotionally traumatic conditions.

¹The seventh building was a hotel.

²According to another study by the Insurance Information Institute, *One Hundred Minutes of Terror That Changed the Global Insurance Industry Forever*, the total value of insurance claims for this event will be about \$40 billion. This study estimated that about \$2.7 billion, or 6.7 percent of this amount, would be for life insurance claims, and the remaining \$37 billion to be for nonlife insurance claims, which include property damages, business interruption, and nonaviation liability claims.

The dust and debris from the attacks and the subsequent collapse of the various World Trade Center structures covered an extensive area of lower Manhattan, up to a mile beyond the center of the attacks, as shown in figure 3.

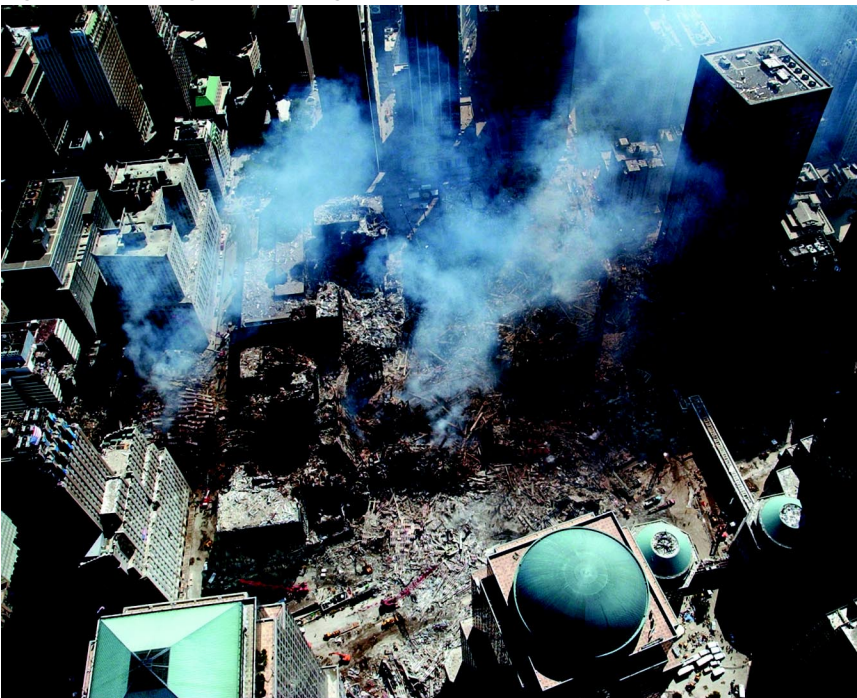
Figure 3: Geographic Extent of Damage and Debris from Attacks in Lower Manhattan



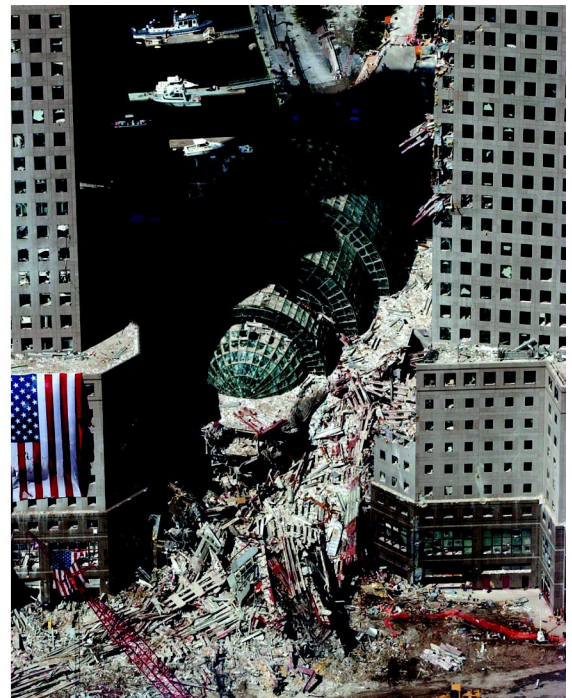
Source: Risk Management Solutions, Inc., "World Trade Center Disaster Special Report," Sept. 18, 2001.

Figures 4 and 5 include various photographs that illustrate the damage to buildings from the towers' collapse and from the dust and debris that blanketed the surrounding area.

Figure 4: Damage to Buildings from Attacks and Resulting Debris



Source: Associated Press.



Left: An aerial view, September 17, 2001, of where the World Trade Center collapsed following the September 11 terrorist attack. Surrounding buildings were heavily damaged by the debris and massive force of the falling twin towers. Right: The debris-clogged Winter Garden between the buildings of the World Financial Center near the World Trade Center. These surrounding buildings, which contained important facilities of various financial market participants, were heavily damaged by the falling twin towers.

Figure 5: Dust and Debris Resulting from Attack



Source: Associated Press.

Left: Police officers and civilians run away from New York's World Trade Center after an additional explosion rocked the buildings Tuesday morning, September 11, 2001. This cloud of dust and debris was estimated to be as much as 30 stories high and blanketed the surrounding area, including financial market organizations' facilities. Top right: Ash covers a street in downtown New York City after the collapse of the World Trade Center. Bottom right: Rubble and ash fill lower Manhattan streets.

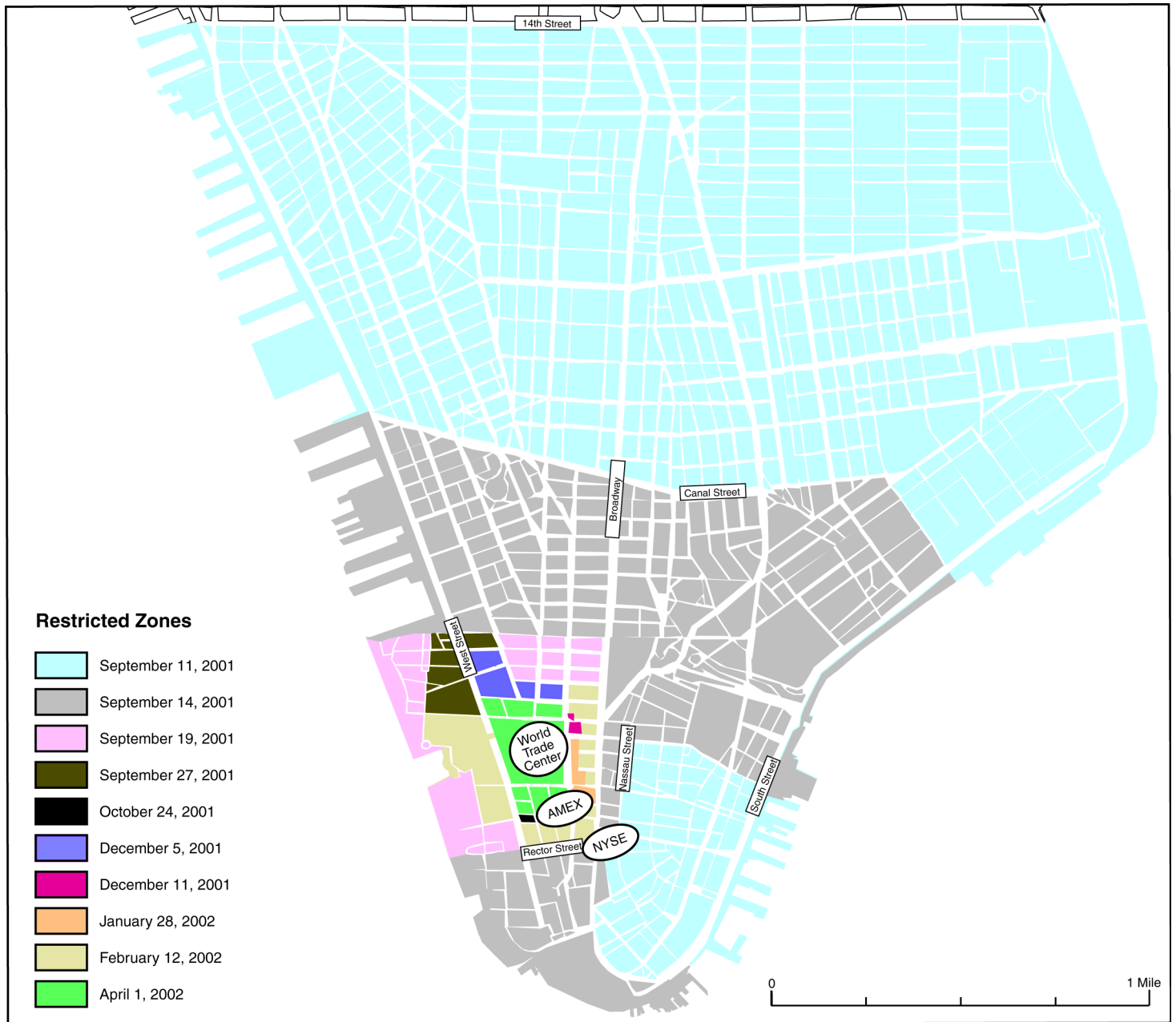
This dust and debris created serious environmental hazards that resulted in additional damage to other facilities and hampered firms' ability to restore operations in the area. For example, firms with major data processing centers could not operate computer equipment until the dust levels had been substantially reduced because of the sensitivity of this equipment to dust contamination. In addition, dust and other hazardous materials made

working conditions in the area difficult and hazardous. According to staff of one of the infrastructure providers with whom we met, the entire area near the World Trade Center was covered with a toxic dust that contained asbestos and other hazardous materials.

Restrictions on physical access to lower Manhattan, put into place after the attacks, also complicated efforts to restore operations. To facilitate rescue and recovery efforts and maintain order, the mayor ordered an evacuation of lower Manhattan, and the New York City Office of Emergency Management restricted all pedestrian and vehicle access to most of this area from September 11 through September 13, 2001. During this time, access to the area was only granted to persons with the appropriate credentials. Federal and local law enforcement agencies also restricted access because of the potential for additional attacks and to facilitate investigations at the World Trade Center site. Figure 6 shows the areas with access restrictions in the days following the attacks.

Chapter 2
September 11 Attacks Severely Disrupted
U.S. Financial Markets

Figure 6: Lower Manhattan Area Subject to Access Restrictions Following September 11, 2001, Attacks



Source: City of New York Emergency Mapping Center.

Some access restrictions were lifted beginning September 14, 2001; however, substantial access restrictions were in place through September 18. From September 19, most of the remaining restrictions were to cordon off the area being excavated and provide access for heavy machinery and emergency vehicles.

Damage from Attacks Significantly Disrupted Telecommunications and Power

The September 11 terrorist attacks extensively damaged the telecommunications infrastructure serving lower Manhattan, disrupting voice and data communications services throughout the area. (We discuss the impact of the attacks on telecommunications infrastructure and telecommunications providers' recovery efforts in more detail in appendix I of this report.) Most of this damage occurred when 7 World Trade Center, itself heavily damaged by the collapse of the twin towers, collapsed into a major telecommunications center at 140 West Street operated by Verizon, the major telecommunications provider for Manhattan. The collateral damage inflicted on that Verizon central office significantly disrupted local telecommunications services to approximately 34,000 businesses and residences in the surrounding area, including the financial district.³ Damage to the facility was compounded when water from broken mains and fire hoses flooded cable vaults located in the basement of the building and shorted out remaining cables that had not been directly cut by damage and debris. As shown in figure 7, the damage to this key facility was extensive.

³A central office is a telephone company facility containing the switching equipment linking customers with public voice and data networks within and outside of the local service area.

Figure 7: Damage to Verizon Central Office at 140 West Street



Source: Verizon Communications, Inc.

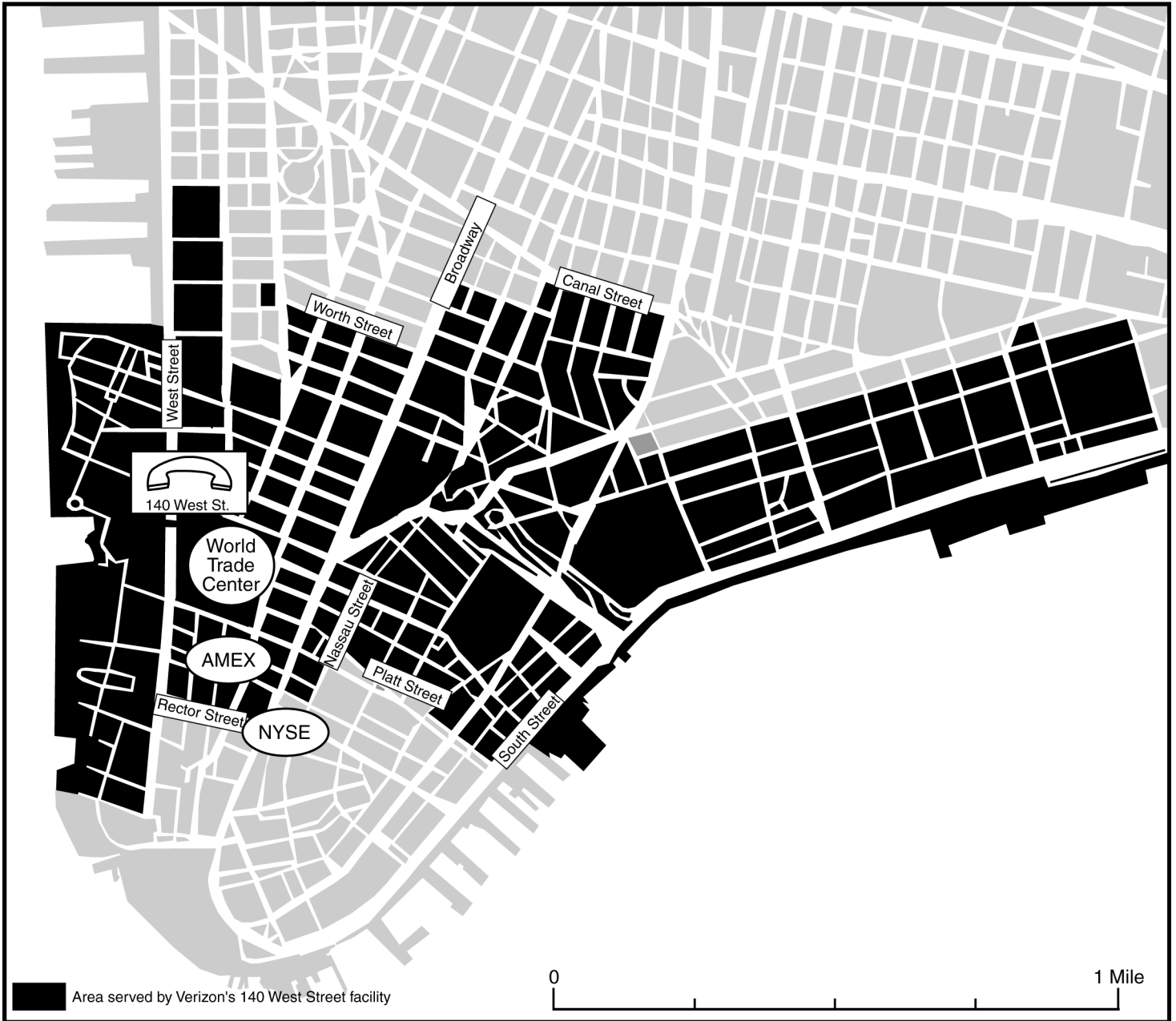
The remains of 7 World Trade Center building rest against the east wall of Verizon's 140 West Street facility. Telecommunications equipment in Verizon's facility also was damaged as a result of efforts to fight the fires burning in 7 World Trade Center. Firefighters used the building to assist in extinguishing adjacent fires. The rubble prevented Verizon technicians from getting into at least 15 manholes to assess and repair cables that run beneath ground zero. Inset top: View of damaged cable vault from street level. Because the cable vault at West Street was crushed, those physical connections between West Street switching facilities and customer premises were lost, resulting in a loss of dial tone for anyone at the World Trade Center and other local customers in the West Street serving area. Inset bottom: View of damaged digital switching system near breached seventh floor of east wall of 140 West Street. These switches were restored to service as a temporary measure but were to be replaced due to contamination.

Because of the damage to Verizon facilities and equipment, significant numbers of customers lost telecommunications services for extended periods. When Verizon's 140 West Street central office was damaged, about 182,000 voice circuits, more than 1.6 million data circuits, almost 112,000 private branch exchange (PBX) trunks, and more than 11,000 lines serving

Internet service providers were lost.⁴ As shown in figure 8, this central office served a large part of lower Manhattan.

⁴A PBX is an automatic telephone switching system that is owned, operated, and located within a private enterprise. This system switches calls between enterprise users on local lines while allowing all users to share a certain number of external telephone lines. A PBX trunk line connects the PBX to the serving telecommunications carrier's local central office switch.

Figure 8: Area Served by Verizon 140 West Street Central Office



Source: Verizon Communications, Inc.

The attacks also damaged other Verizon facilities and affected customers in areas beyond that served directly from the Verizon West Street central office. Three other Verizon switches in the World Trade Center towers and in 7 World Trade Center were also destroyed in the attacks. Additional services were disrupted because 140 West Street also served as a transfer station on the Verizon network for about 2.7 million circuits carrying data traffic that did not originate or terminate in that serving area, but that nevertheless passed through that particular physical location. For example, communications services provided out of the Verizon Broad Street central office that passed through West Street were also disrupted until new cabling could be put in place to physically carry those circuits around the damaged facility. As a result, a total of about 4.4 million Verizon data circuits had to be restored.

Other telecommunications carriers that serviced customers in the affected area also experienced damage and service disruptions. For example, in 140 West Street, 30 telecommunications providers had equipment that linked their networks to Verizon. Other firms lost even more equipment than Verizon. For example, AT&T lost a key transmission facility that serviced its customers in lower Manhattan and had been located in one of the World Trade Center towers.

The attacks also caused major power outages in lower Manhattan. Con Edison, the local power provider, lost three power substations and more than 33 miles of cabling; total damage to the power infrastructure was estimated at \$410 million. As a result, more than 13,000 Con Edison business customers lost power, which required them to either relocate operations or use alternative power sources such as portable generators.

To restore telecommunications and power, service providers had to overcome considerable challenges. Access restrictions made this work more difficult—staff from WorldCom told us that obtaining complete clearance through the various local, state, and federal officials, including the National Guard, took about 2 days. In some cases, environmental and other factors also prevented restoration efforts from beginning. According to Verizon staff, efforts to assess the damage and begin repairs on 140 West Street initially were delayed by concerns over the structural integrity of the damaged facility and other nearby buildings; several times staff had to halt assessment and repair efforts because government officials ordered evacuations of the building.

In some cases, infrastructure providers employed innovative solutions to restore telecommunications and power quickly. For example, these providers placed both telecommunications and power cables that are normally underground directly onto the streets and covered them with temporary plastic barriers. Con Edison repair staff also had tanks of liquid nitrogen placed on street corners so that their employees could freeze cables, which makes them easier to cut when making repairs. To work around the debris that blocked access to 140 West, Verizon staff ran cables over the ground and around damaged cabling to quickly restore services. Because of damage to the reinforced vault that previously housed the cables at Verizon's facility, a new cable vault was reconstructed on the first floor, and cables were run up the side of the building to the fifth and eighth floors, as shown in figure 9.

Figure 9: Verizon Used Temporary Cabling Solutions at 140 West Street



Source: Verizon Communications, Inc.

Verizon restored service by using temporary cabling above and below ground in the days following the attack.

Attacks Severely Affected Financial Markets but Heroic Efforts Were Made to Restore Operations

Although the facilities of the stock and options exchanges and clearing organizations in lower Manhattan were largely undamaged by the attacks, many market participants were affected by the loss of telecommunications and lack of access to lower Manhattan. As a result, many firms, including some of the broker-dealers responsible for significant portions of the overall securities market trading activity, were forced to relocate operations to backup facilities and alternative locations. To resume operations, these new facilities had to be prepared for trading and provided with sufficient telecommunications capacity. Some firms had to have telecommunications restored although they thought they had redundant communications services. Regulators and market participants delayed the opening of the stock and options market until September 17, until the key broker-dealers responsible for large amounts of market liquidity were able to operate and telecommunications had been tested.

Most Securities Exchanges and Market Support Organizations Were Not Directly Damaged

Although several securities exchanges and market support organizations were located in the vicinity of the attacks, most did not experience direct damage. The NYSE, Depository Trust and Clearing Corporation,⁵ Securities Industry Automation Corporation (SIAC), International Securities Exchange, and the Island ECN all had important facilities located in close proximity to the World Trade Center, but none of these organizations' facilities were damaged. The American Stock Exchange (Amex) was the only securities exchange that experienced incapacitating damage.⁶ Amex was several hundred feet from the World Trade Center towers, but sustained mostly broken windows and damage to some offices. However, its drainage and ventilation systems were clogged by dust and debris and the building lost power, telephones, and access to water and steam. The loss of steam and water coupled with the inadequate drainage and ventilation meant that Amex computer systems could not run due to a lack of air conditioning. As a result, the Amex building was not cleared for reoccupation until October 1, 2001, after inspectors had certified the building as structurally sound and power and water had been fully restored. Although the remaining exchanges were not damaged, U.S. stock

⁵The Depository Trust and Clearing Corporation is the holding company for various organizations that conduct clearance and settlement services, including the Depository Trust Company and the National Securities Clearing Corporation.

⁶Several futures exchanges experienced damage, including one whose operations were located in one of the World Trade Center towers.

and options exchanges nationwide closed the day of the attacks and did not reopen until September 17, 2001. However, regulators and market participants acknowledged that if the major exchanges or clearing organizations had sustained damage, trading in the markets would have likely taken longer to resume.

Damage to Financial
Institutions' Facilities and
Telecommunications Forced
Relocations and Made
Recovery Efforts
Challenging

Although most exchanges and market support organizations were not damaged by the attacks, several key firms with substantial operations in the area sustained significant facilities damage. As a result of this damage and the inability to access the area in the days following the attacks, many financial institution participants had to relocate their operations, in some cases using locations not envisioned by their BCPs. They then faced the challenge of recreating their key operations and obtaining sufficient telecommunications services at these new locations. For example, one large broker-dealer with headquarters that had been located across from the World Trade Center moved operations to midtown Manhattan, taking over an entire hotel. To resume operations, firms had to obtain computers and establish telecommunications lines in the rooms that were converted to work spaces. Another large broker-dealer whose facilities were damaged by the attacks attempted to reestablish hundreds of direct lines to its major customers after relocating operations to the facilities of a recently purchased broker-dealer subsidiary in New Jersey. The simultaneous relocation of so many firms meant that they also had to establish connections to the new operating locations of other organizations. Although Verizon managers were unable to estimate how much of its restoration work in the days following the attacks specifically addressed such needs, they told us that considerable capacity was added to the New Jersey area to accommodate many of the firms that relocated operations there, including financial firms.

Restoring operations often required innovative approaches. According to representatives of the exchanges and other financial institutions we spoke with, throughout the crisis financial firms that are normally highly competitive instead exhibited a high level of cooperation. In some cases, firms offered competitors facilities and office space. For example, traders who normally traded stocks on the Amex floor obtained space on the trading floor of NYSE, and Amex options traders were provided space at the Philadelphia Stock Exchange. In some cases, innovative approaches were used by the exchanges and utilities to restore lost connectivity to their customers. For example, technicians at the Island ECN created virtual private network connections for those users whose services were

disrupted.⁷ Island also made some of its trading applications available to its customers through the Internet. In another example, SIAC, which processes trades for NYSE and the American Stock Exchange, worked closely with its customers to reestablish their connectivity, reconfiguring customers' working circuits that had been used for testing or clearing and settlement activities to instead transmit data to SIAC's trading systems.

The Bond Market Association, the industry association representing participants in the government and other debt markets, and the Securities Industry Association (SIA), which represents participants in the stock markets, played critical roles in reopening markets. Both associations helped arrange daily conference calls with market participants and regulators to address the steps necessary to reopen the markets. At times, hundreds of financial industry officials were participating in these calls. These organizations also made recommendations to regulators to provide some relief to their members so that they could focus on restoring their operations. For example, the Bond Market Association recommended to its members that they extend the settlement date for government securities trades from the day following trade date (T+1) to five days after to help alleviate some of the difficulties that were occurring in the government securities markets. Through a series of conference calls with major banks and market support organizations, SIA was instrumental in helping to develop an industrywide consensus on how to resolve operational issues arising from the damage and destruction to lower Manhattan and how to mitigate operational risk resulting from the destruction of physical (that is, paper) securities, which some firms had maintained for customers.

SEC also took actions to facilitate the successful reopening of the markets. To allow market participants to focus primarily on resuming operations, SEC issued rules to provide market participants temporary relief from certain regulatory requirements. For example, SEC extended deadlines for disclosure and reporting requirements, postponed the implementation date for new reporting requirements, and temporarily waived some capital regulation requirements. SEC implemented other relief measures targeted toward stabilizing the reopened markets. For example, SEC relaxed rules that restrict corporations from repurchasing their own shares of publicly

⁷A virtual private network is a private data network that uses public telecommunication infrastructure such as the Internet to provide remote users with secure access to an organization's network.

traded stock, and simplified registration requirements for airline and insurance industries so that they could more easily raise capital.

Stock and Options Markets Opening Was Delayed until Sufficient Connectivity and Liquidity Existed

Partially because of the difficulties experienced by many firms in restoring operations and obtaining adequate telecommunications service, the reopening of the markets was delayed. Although thousands of broker-dealers may participate in the securities markets, staff at NYSE and NASDAQ told us that a small number of firms account for the majority of the trading volume on their markets. Many of those firms had critical operations in the area affected by the attacks. For example, 7 of the top 10 broker-dealers ranked by capital had substantial operations in the World Trade Center or the World Financial Center, across from the World Trade Center. In the immediate aftermath of the attack, these and other firms were either attempting to restore operations at their existing locations or at new locations. In addition, financial market participant staff and the financial regulators told us that their staffs did not want to return to the affected area too soon to avoid interfering with the rescue and recovery efforts. For example, the SEC Chairman told us that he did not want to send 10,000 to 15,000 workers into lower Manhattan while the recovery efforts were ongoing and living victims were still being uncovered.

Because of the considerable efforts required for broker-dealers to restore operations, insufficient liquidity existed to open the markets during the week of the attacks. According to regulators and exchange staff, firms able to trade by Friday, September 14, accounted for only about 60 percent of the market's normal order flow. As a result, securities regulators, market officials, and other key participants decided that, until more firms were able to operate normally, insufficient liquidity existed in the markets. Opening the markets with some firms but not others was also viewed as unfair to many of the customers of the affected firms. Although institutional clients often have relationships with multiple broker-dealers, smaller customers and individual investors usually do not; thus, they may not have been able to participate in the markets under these circumstances.

In addition, connectivity between market participants and exchanges had not been tested. For this reason, it was unclear how well the markets would operate when trading resumed because so many critical telecommunication connections were damaged in the attacks and had been either repaired or replaced. Staff from the exchanges and market participants told us that the ability to conduct connectivity testing prior to

the markets reopening was important. Many firms experienced technical difficulties in getting the new connections they had obtained to work consistently as telecommunication providers attempted to restore telecommunications service. According to officials at one exchange, restoring connections to its members was difficult because existing or newly restored lines that were initially operational would erratically lose their connectivity throughout the week following September 11. Representatives of the exchanges and financial regulators with whom we met told us that opening the markets but then having to shut them down again because of technical difficulties would have greatly reduced investor confidence.

Because of the need to ensure sufficient liquidity and a stable operating environment, market participants and regulators decided to delay the resumption of stock and options trading until Monday, September 17. This delay allowed firms to complete their restoration efforts and use the weekend to test connectivity with the markets and the clearing organizations. As a result of these efforts, the stock and options markets reopened on September 17 and traded record volumes without significant operational difficulties.

Disruptions in Government Securities and Money Markets Severely Affected Clearance and Settlement, Liquidity, and Trade Volumes

The attacks also severely disrupted the markets for government securities and money market instruments primarily because of the impact on the broker-dealers that trade in the market and on one of the key banks that perform clearing functions for these products. According to regulatory officials, at the time of the attacks, eight of the nine IDBs, which provide brokerage services to other dealers in government securities, had operations that were severely disrupted following the attacks. The most notable was Cantor Fitzgerald Securities, whose U.S. operations had been located on several of the highest floors of one of the World Trade Center towers. Because much of the trading in the government securities market occurs early in the day, the attacks and subsequent destruction of the towers created massive difficulties for this market. When these IDBs' facilities were destroyed, the results of trading, including information on which firms had purchased securities and which had sold, also were largely lost. These trades had to be reconstructed from the records of the dealers who had conducted trades with the IDBs that day. In addition, with the loss of their facilities, most of the primary IDBs were not able to communicate with the Government Securities Clearing Corporation (GSCC), which also complicated the clearing and settlement of these trades. Staff from

financial market participants told us that reconciling some of these transactions took weeks, and in some cases, months.

Two banks—the Bank of New York (BONY) and JP Morgan Chase—were the primary clearing banks for government securities. Clearing banks are essentially responsible for transferring funds and securities for their dealer and other customers that purchase or sell government securities. For trades cleared through GSCC, the clearing organization for these instruments, instructs its dealer members and the clearing banks as to the securities and associated payments to be transferred to settle its members' net trade obligations.

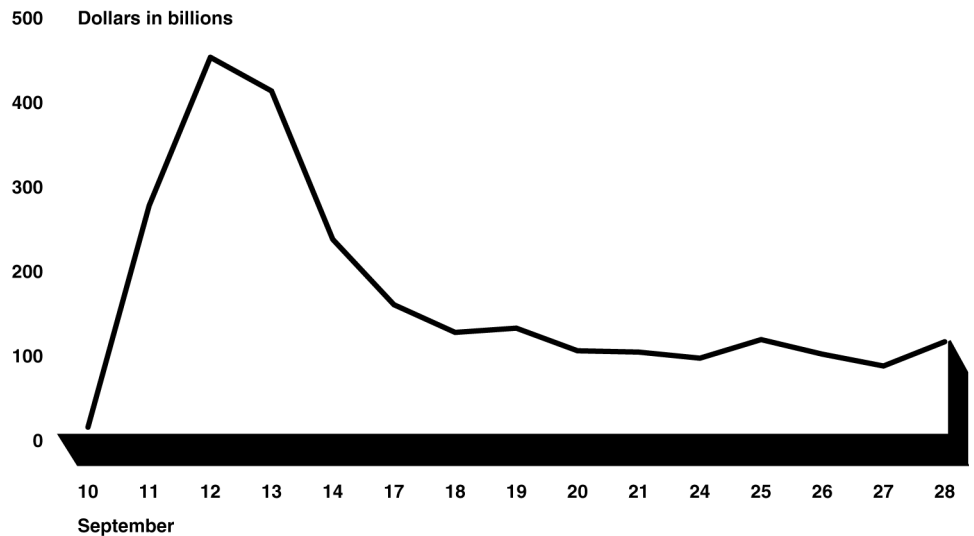
As a result of the attacks, BONY and its customers experienced telecommunications and other problems that contributed to the disruption in the government securities market because it was the clearing bank for many major market participants and because it maintained some of GSCC's settlement accounts. BONY had to evacuate four facilities including its primary telecommunications data center and over 8,300 staff, because they were located near the World Trade Center.

At several of these facilities, BONY conducted processing activities as part of clearing and settling government securities transactions on behalf of its customers and GSCC. The communication lines between BONY and the Fedwire systems for payment and securities transfers, as well as those between BONY and its clients, were critical to BONY's government securities operations. Over these lines, BONY transmitted data with instructions to transfer funds and securities from its Federal Reserve accounts to those of other banks for transactions in government securities and other instruments. BONY normally accessed its Federal Reserve accounts from one of the lower Manhattan facilities that had to be abandoned. In the days following the attacks, BONY had difficulties in reestablishing its Fedwire connections and processing transactions. In addition, many BONY customers also had to relocate and had their own difficulties in establishing connections to the BONY backup site. As a result of these internal processing problems and inability to communicate with its customers, BONY had problems determining what amounts should be transferred on behalf of the clients for whom it performed clearing services. For example, by September 12, 2001, over \$31 billion had been transferred to BONY's Federal Reserve account for GSCC, but because BONY could not access this account, it could not transfer funds to which its clients were entitled. BONY was not able to establish connectivity with

GSCC and begin receiving and transmitting instructions for payment transfers until September 14, 2001.

The problems at the IDBs and BONY affected the ability of many government securities and money markets participants to settle their trades. Before a trade can be cleared and settled, the counterparties to the trade and the clearing banks must compare trade details by exchanging messages to ensure that each is in agreement on the price and amount of securities traded. To complete settlement, messages then must be exchanged between the parties to ensure that the funds and ownership of securities are correctly transferred. If trade information is not correct and funds and securities are not properly transferred, the trade will be considered a “fail.” As shown in figure 10, failed transactions increased dramatically, rising from around \$500 million per day to over \$450 billion on September 12, 2001. The level of fails also stayed high for many days following the attacks, averaging about \$100 billion daily through September 28.

Figure 10: Failed Transactions in the Government Securities Markets During September 2001



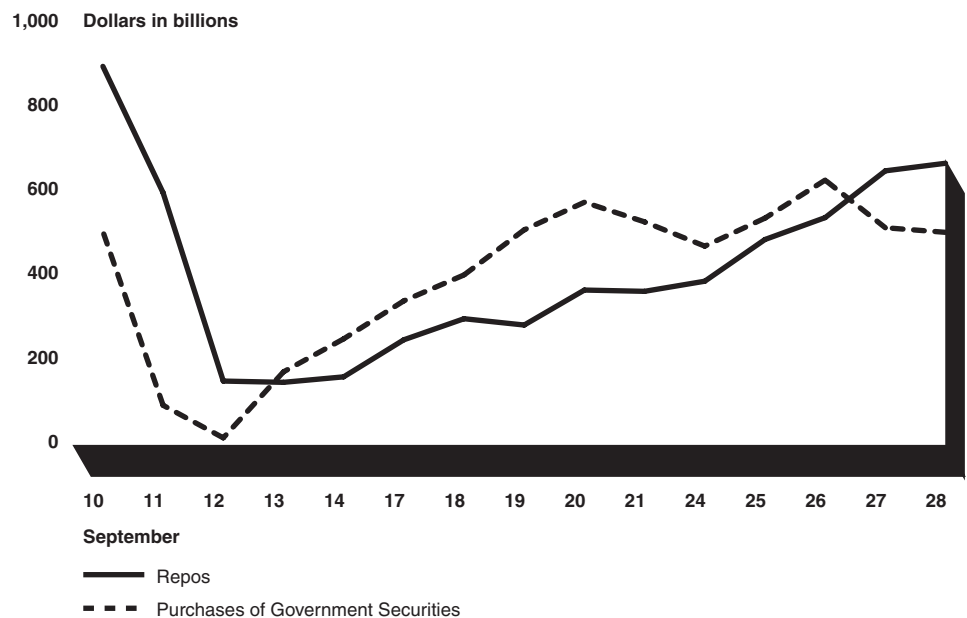
Source: GSCC.

The problems in the government securities markets also created liquidity problems for firms participating in and relying on these markets to fund their operations. Many firms, including many large broker-dealers, fund

their operations using repurchase agreements, or repos, in which one party sells government securities to another party and agrees to repurchase those securities on a future date at a fixed price. Because repos are used to finance firms' daily operations, many of these transactions are executed before 9:00 a.m. As a result, by the time the attacks occurred on September 11, over \$500 billion in repos had been transacted. With so many IDB records destroyed, many of the transactions could not be cleared and settled, causing many of these transactions to fail. As a result, some firms that relied on this market as a funding source experienced major funding shortfalls.

Although trading government securities was officially resumed within 2 days of the attacks, overall trading activity was low for several days. For example, as shown in figure 11, trading volumes went from around \$500 billion on September 10 to as low as \$9 billion on September 12, 2001. Similarly, repo activity fell from almost \$900 billion on September 10 to \$145 billion on September 13.

Figure 11: Cash Purchases of Government Securities and Repo Market Activity During September 2001



Source: GSCC.

The attacks also disrupted the markets for commercial paper, which are short-term securities issued by financial and other firms to raise funds. According to clearing organization officials, the majority of commercial paper redemptions—when the investors that originally purchased the commercial paper have their principal returned— that were scheduled to be redeemed on September 11 and September 12 were not paid until September 13. Firms that relied on these securities to fund their operations had to obtain other sources of funding during this period.

The Federal Reserve took several actions to mitigate potential damage to the financial system resulting from liquidity disruptions in these markets. Banking regulatory staff told us that the attacks largely resulted in a funding liquidity problem rather than a solvency crisis for banks. Thus, the challenge they faced was ensuring that banks had adequate funds to meet their financial obligations. The settlement problems also prevented broker-dealers and others from using the repo markets to fund their daily operations. Soon after the attacks, the Federal Reserve announced that it would remain open to help banks meet their liquidity needs. Over the next 4 days, the Federal Reserve provided about \$323 billion to banks through various means to overcome the problems resulting from unsettled government securities trades and financial market dislocations. For example, from September 11 through September 14, the Federal Reserve loaned about \$91 billion to banks through its discount window, in contrast to normal lending levels of about \$100 million.⁸ It also conducted securities purchase transactions and other open market operations of about \$189 billion to provide needed funds to illiquid institutions. Had these actions not been taken, some firms unable to receive payments may not have had sufficient liquidity to meet their other financial obligations, which could have produced other defaults and magnified the effects of September 11 into a systemic solvency crisis.

Regulators also took action to address the failed trades resulting from the attacks. From September 11 through September 13, the Federal Reserve loaned \$22 billion of securities from its portfolio to broker-dealers that needed securities to complete settlements of failed trades. According to Federal Reserve staff, the Federal Reserve subsequently reduced restrictions on its securities lending that led to a sharp increase in

⁸The discount window is the lending mechanism used by the Federal Reserve Banks to lend funds to depository institutions on a short-term basis to cover temporary liquidity needs or reserve deficiencies.

borrowings at the end of September 2001. Treasury also played a role in easing the failed trades and preventing a potential financial crisis by conducting an unplanned, special issuance of 10-year notes to help address a shortage of notes of this duration in the government securities markets. Market participants typically use these securities as collateral for financing or to meet settlement obligations.

To provide dollars needed by foreign institutions, the Federal Reserve also conducted currency swaps with the Bank of Canada, the European Central Bank, and the Bank of England. The swaps involved exchanging dollars for the foreign currencies of these jurisdictions, with agreements to re-exchange amounts later. These temporary arrangements provided funds to settle dollar-denominated obligations of foreign banks whose U.S. operations were affected by the attacks.

The Federal Reserve, Federal Deposit Insurance Corporation, OCC, and the Office of Thrift Supervision issued a joint statement after the attacks to advise the institutions they oversee that any temporary declines in capital would be evaluated in light of the institution's overall financial condition. The Federal Reserve also provided substantial amounts of currency so that banks would be able to meet customer needs.

Impact of Attacks on the Banking and Payments Systems Was Less Severe

With a few exceptions, commercial banks were not as adversely affected as broker-dealers by the attacks. Although some banks had some facilities and operations in lower Manhattan, they were not nearly as geographically concentrated as securities market participants. As discussed previously, BONY was one bank with significant operations in the World Trade Center area, but only a limited number of other large banks had any operations that were affected. According to regulatory officials that oversee national banks, seven of their institutions had operations in the areas affected by the attacks.

Most payment system operations continued with minimal disruption. The Federal Reserve Bank of New York (FRBNY) manages the Federal Reserve's Fedwire securities and payments transfer systems. Although the FRBNY sustained damage to some telecommunications lines, Fedwire continued processing transactions without interruption because the actual facilities that process the transactions are not located in lower Manhattan. However, Federal Reserve officials noted that some banks experienced problems connecting to Fedwire because of the widespread damage to telecommunications systems. Over 30 banks lost connectivity to Fedwire

because their data first went to the FRBNY facility in lower Manhattan before being transmitted to Fedwire's system's processing facility outside the area. However, most were able to reestablish connections through dial-up backup systems and some began reporting transfer amounts manually using voice lines. Federal Reserve officials noted that normal volumes for manually reported transactions were about \$200–\$400 million daily, but from September 11 through September 13, 2001, banks conducted about \$151 billion in manually reported transactions. A major private-sector payments system, CHIPS, also continued to function without operational disruptions, although 19 of its members temporarily lost connectivity with CHIPS in the aftermath of the attacks and had to reconnect from backup facilities.

Retail payments systems, including check clearing and automated clearing house transactions, generally continued to operate. However, the grounding of air transportation did complicate and delay some check clearing, since both the Federal Reserve and private providers rely on overnight air delivery to transport checks between banks in which they are deposited and banks from which they are drawn.⁹ Federal Reserve officials said they were able to arrange truck transportation between some check clearing offices until they were able to gain approval for their chartered air transportation to resume several days later. According to Federal Reserve staff, transporting checks by ground slowed processing and could not connect all offices across the country. The staff said that the Federal Reserve continued to credit the value of deposits to banks even when it could not present checks and debit the accounts of paying banks. This additional liquidity—normally less than \$1 billion—peaked at over \$47 billion on September 13, 2001.

⁹The Expedited Funds Availability Act of 1987, which is implemented through Federal Reserve Board Regulation CC, requires that banks make funds available for withdrawal within 2 days when the bank of first deposit and the paying bank are located within the same Federal Reserve check processing territory and within 5 days when the banks are not in the same territory. Meeting those deadlines frequently requires air transport of checks.

Attacks Revealed Limitations in Financial Market Participants' Business Continuity Capabilities

The terrorist attacks revealed that limits that existed in market participants' business continuity capabilities at the time of the attacks. Based on our discussions with market participants, regulators, industry associations and others, the BCPs of many organizations had been too limited in scope to address the type of disaster that occurred. Instead, BCPs had procedures to address disruptions affecting a single facility such as power outages or fires at one building. For example, a 1999 SEC examination report of a large broker-dealer that we reviewed noted that in the event of an emergency this firm's BCP called for staff to move just one-tenth of a mile to another facility. By not planning for wide-scale events, many organizations had not invested in backup facilities that could accommodate key aspects of their operations, including several of the large broker-dealers with primary operations located near the World Trade Center that had to recreate their trading operations at new locations. Similarly, NYSE and several of the other exchanges did not have backup facilities at the time of the attacks from which they could conduct trading.

The attacks also illustrated that some market participants' backup facilities were too close to their primary operations. For example, although BONY had several backup facilities for critical functions located several miles from the attacks, the bank also backed up some critical processes at facilities that were only blocks away. According to clearing organization and regulatory staff, one of the IDBs with facilities located in one of the destroyed towers of the World Trade Center had depended on backup facilities in the other tower.

Additionally, firms' BCPs did not adequately take into account all necessary equipment and other resources needed to resume operations as completely and rapidly as possible. For example, firms that occupied backup facilities or other temporary space found that they lacked sufficient space for all critical staff or did not have all the equipment needed to conduct their operations. Others found that their backup sites did not have the most current versions of the software and systems that they use, which caused some restoration problems. Some firms had contracted with third-party vendors for facilities and equipment to conduct operations during emergencies, but because so many firms were disrupted by the attacks, some of these facilities were overbooked, and firms had to find other locations in which to resume operations.

Organizations also learned that their BCPs would have to better address human capital issues. For example, some firms had difficulties in locating

key staff in the confusion after the attacks. Others found that staff were not able to reach their backup locations as quickly as their plans had envisioned due to the closure of public transit systems, bridges, and roads. Other firms had not planned for the effects of the trauma and grief on their staff and had to provide access to counseling for those that were overwhelmed by the events.

The attacks also revealed the need to improve some market participants' business continuity capabilities for telecommunications. According to broker-dealers and regulator staff with whom we spoke, some firms found that after relocating their operations, they learned that their backup locations connected to the primary sites of the organizations critical to their operations but not to these organizations' backup sites. Some financial firms that did not have damaged physical facilities nonetheless learned that their supporting telecommunications services were not as diverse and redundant as they expected. Diversity involves establishing different physical routes in and out of a building, and using different equipment along those routes if a disaster or other form of interference adversely affects one route. Redundancy involves having extra capacity available, generally from more than one source, and also incorporates aspects of diversity. Therefore, users that rely on telecommunications services to support important applications try to ensure that those services use facilities that are diverse and redundant so that no single point in the communications path can cause all services to fail. Ensuring that carriers actually maintain physically redundant and diverse telecommunications services has been a longstanding concern within the financial industry. For example, the President's National Security Telecommunications Advisory Committee in December 1997 reported, "despite assurances about diverse networks from the carriers, a consistent concern among the financial services industry was the trustworthiness of their telecommunications diversity arrangements."¹⁰

This concern was validated following the September 11 attacks when firms that thought they had achieved redundancy in their communications systems learned that their network services were still disrupted. According to regulators and financial market participants with whom we spoke, some firms that made arrangements with multiple service providers to obtain redundant service discovered that the lines used by their providers were

¹⁰The President's National Security Telecommunications Advisory Committee, *Financial Services Risk Assessment Report* (Washington, D.C.: December 1997).

not diverse because they routed through the same Verizon switching facility. Other firms that had mapped out their communications lines to ensure that their lines flowed through physically diverse paths at the time those services were first acquired found that their service providers had rerouted some of those lines over time without their knowledge, eliminating that assurance of diversity in the process.

Observations

The attacks demonstrated that the ability of U.S. financial markets to remain operational after disasters depends to a great extent on the preparedness of not only the exchanges and clearing organizations but also the major broker-dealers and banks that participate in these markets. The various financial markets were severely affected and the stock and options exchanges were closed in the days following the attacks for various reasons, including the need to conduct rescue operations. However, the markets also remained closed because of the time required for several major broker-dealers that normally provide the bulk of the liquidity for trading in the stock, options, and government securities markets to become operational. Although the attacks were of a nature and magnitude beyond that previously imagined, they revealed the need to address limitations in the business continuity capabilities of many organizations and to mitigate the concentration of critical operations in a limited geographic area. Many organizations will have to further assess how vulnerable their operations are to disruptions and determine what capabilities they will need to increase the likelihood of being able to resume operations after such events.

Financial Market Participants Have Taken Actions to Reduce Risks of Disruption, but Some Limitations Remain

Since the attacks, exchanges, clearing organizations, ECNs, and payment system processors implemented various physical and information security measures and business continuity capabilities to reduce the risk that their operations would be disrupted by attacks, but some organizations continued to have limitations in their preparedness that increases their risk of disruption. With threats to the financial markets potentially increasing, organizations must choose how best to use their resources to reduce risks by investing in protection against physical and electronic attacks for facilities, personnel, and information systems and developing capabilities for continuing operations. To reduce the risk of operations disruptions, the 15 financial market organizations—including the 7 critical ones—we reviewed in 2002 had taken many steps since the attacks to protect their physical facilities or information systems from attacks and had developed plans for recovering from such disruptions. However, at the time we conducted our review, 9 of the 15 organizations, including 2 we considered critical to the functioning of the financial markets, had not taken steps to ensure that they would have the staff necessary to conduct their critical operations if the staff at their primary site were incapacitated—including 8 organizations that also had physical vulnerabilities at their primary sites. Ten of the 15 organizations, including 4 of the critical organizations, also faced increased risk of being unable to operate after a wide-scale disruption because they either lacked backup facilities or had backup facilities near their primary sites. Finally, although many of the 15 organizations had attempted to reduce their risks by testing some of their risk reduction measures, only 3 were testing their physical security measures, only 8 had recently assessed the vulnerabilities of their key information systems, and only 7 had fully tested their BCPs.

In Climate of Increasing Risk, Organizations Often Have to Choose How to Best Use Resources

Faced with varying and potentially increasing threats that could disrupt their operations, organizations must make choices about how to best use their resources to both protect their facilities and systems and develop business continuity capabilities. September 11, 2001, illustrated that such attacks can have a large-scale impact on market participants. Law enforcement and other government officials are concerned that public and private sectors important to the U.S. economy, including the financial markets, may be increasingly targeted by hostile entities that may have increasing abilities to conduct such attacks. For example, the leader of the al Qaeda organization was quoted as urging that attacks be carried out against the “pillars of the economy” of the United States. Press accounts of captured al Qaeda documents indicated that members of this organization may be increasing their awareness and knowledge of electronic security

techniques and how to compromise and damage information networks and systems, although the extent to which they could successfully conduct sophisticated attacks has been subject to debate. A recent report on U.S. foreign relations also notes that some foreign countries are accelerating their efforts to be able to attack U.S. civilian communications systems and networks used by institutions important to the U.S. economy, including those operated by stock exchanges.¹

The physical threats that individual organizations could reasonably be expected to face vary by type and likelihood of occurrence. For example, events around the world demonstrate that individuals carrying explosive devices near or inside facilities can be a common threat. More powerful explosive attacks by vehicle are less common but still have been used to devastating effect in recent years. Other less likely, but potentially devastating, physical threats include attacks involving biological or chemical agents such as the anthrax letter mailings that occurred in the United States in 2001 and the release of a nerve agent in the Tokyo subway in 1995.

Faced with the potential for such attacks, organizations can choose to invest in a range of physical security protection measures to help manage their risks. The Department of Justice has developed standards that identify measures for protecting federal buildings from physical threats.² To reduce the likelihood of incurring damage from individuals or explosives, organizations can physically secure perimeters by controlling vehicle movement around a facility, using video monitoring cameras, increasing lighting, and installing barriers. Organizations can also prevent unauthorized persons or dangerous devices from entering their facilities by screening people and objects, restricting lobby access, and only allowing employees or authorized visitors inside. Organizations could also take steps to prevent biological or chemical agents from contaminating facilities by opening and inspecting mail and deliveries off-site. To protect sensitive

¹U.S.-China Security Review Commission, *Report to Congress of the U.S.-China Security Review Commission: The National Security Implications of the Economic Relationships Between the United States and China* (July 2002).

²See Department of Justice, *Vulnerability Assessment of Federal Facilities* (Washington, D.C.: Jun. 28, 1995). This document presented security standards to be applied to all federal facilities. Each facility is to be placed in five categories depending on its level of risk, with Level 1 facilities having the least need for physical security and Level 5 facilities having the highest need. Based on its risk level, a facility would be expected to implement increasingly stringent measures in 52 security areas.

data, equipment, and personnel, organizations can also take steps to secure facility interiors by using employee and visitor identification systems and restricting access to critical equipment and utilities such as power and telecommunications equipment.

Organizations can also reduce the risk of operations disruptions by investing in measures to protect information systems. Information system threats include hackers, who are individuals or groups attempting to gain unauthorized access to networks or systems to steal, alter, or destroy information. Another threat—known as a denial of service attack— involves flooding a system with messages that consume its resources and prevent authorized users from accessing it. Information systems can also be disrupted by computer viruses that damage data directly or degrade system performance by taking over system resources. Information security guidance used for reviews of federal organizations recommend that organizations develop policies and procedures that cover all major systems and facilities and outline the duties of those responsible for security.³ To prevent unauthorized access to networks and information systems, organizations can identify and authenticate users by using software and hardware techniques such as passwords, firewalls, and other filtering devices. Organizations can also use monitoring systems to detect unauthorized attempts to gain access to networks and information systems and develop response capabilities for electronic attacks or breaches.

Investing in business continuity capabilities is another way that organizations can reduce the risk that their operations will be disrupted. According to guidance used by private organizations and financial regulators, developing a sound BCP requires organizations to determine which departments, business units, or functions are critical to operations.⁴ The organizations should then prepare a BCP that identifies capabilities that have to be in place, resources required, and procedures to be followed for the organization to resume operations. Such capabilities can include backup facilities equipped with the information technology hardware and software that the organization needs to conduct operations. Alternatively, organizations can replace physical locations or processes, such as trading

³U.S. General Accounting Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

⁴Among the sources we consulted were our own 1999 *Federal Information System Controls Audit Manual* (FISCAM), the FFIEC *Information Systems Handbook: Volume 1*, and the Business Continuity Institute's 2001 *Business Guide to Continuity Management*.

floors, with electronic systems that perform the same core functions. Many organizations active in the financial markets are critically dependent on telecommunications services for transmitting the data or voice traffic necessary to operate. As a result, organizations would have to identify their critical telecommunications needs and take steps to ensure that services needed to support critical operations will be available after a disaster. Finally, BCP guidance such as FISCAM, which provides standards for audits of federal information systems, also recommends that organizations have backup staff that can implement BCP procedures. To the extent that an organization's ability to resume operations depends on the availability of staff with specific expertise, the organization has to maintain staff capable of conducting its critical functions elsewhere.

Given that most organizations have limited resources, effectively managing the risk of operations disruptions involves making trade-offs between investing in protection of facilities, personnel, and systems or development of business continuity capabilities. For example, organizations must weigh the expected costs of operations disruptions against the expected cost of implementing security protections, developing facilities, or implementing other business continuity capabilities to ensure that they would be able to resume operations after a disaster. Risk management guidance directs organizations to identify how costly various types of temporary or extended outages or disruptions would be to parts or all of their operations. Such costs stem not only from revenues actually lost during the outage, but also from potential lost income because of damage to the organization's reputation stemming from its inability to resume operations. In addition to estimating the potential costs of disruptions, organizations are advised to identify potential threats that could cause such disruptions and estimate the likelihood of these events. By quantifying the costs and probabilities of occurrence of various disruptions, an organization can then better evaluate the amount and how to allocate the resources that it should expend on either implementing particular protection measures or attaining various business continuity capabilities. For example, an organization whose primary site is located in a highly trafficked, public area may have limited ability to reduce all of its physical security risks. However, such an organization could reduce the risk of its operations being disrupted by having a backup facility manned by staff capable of supporting its critical operations or by cross-training other staff.

All Financial Market Organizations Were Taking Steps to Reduce the Risks of Operations Disruptions

The 15 exchanges, clearing organizations, ECNs, and payment system processors we reviewed in 2002 had invested in various physical and information protections and business continuity capabilities to reduce the risk that their operations would be disrupted. Each of these 15 organizations had implemented physical security measures to protect facilities and personnel. To establish or increase perimeter security, some organizations had erected physical barriers around their facilities such as concrete barriers, large flowerpots, or boulders. To reduce the likelihood that its operations would be disrupted by vehicle-borne explosives, one organization had closed off streets adjacent to its building and had guards inspect all vehicles entering the perimeter. Some organizations were also using electronic surveillance to monitor their facilities, with some organizations having 24-hour closed circuit monitoring by armed guards. Others had guards patrolling both the interior and exterior of their facilities on a 24-hour basis. In addition, all of these organizations had taken measures to protect the security of their interiors. For example, the organizations required employee identification, electronic proximity cards, or visitor screening.

All 15 organizations had taken measures to reduce the risk that electronic threats would disrupt their operations. The securities markets already use networks and information systems that reduce their vulnerability to external intrusion in several ways. First, the securities exchanges and clearing organizations have established private networks that transmit traffic only to and from their members' systems, which are therefore more secure than the Internet or public telephone networks. Second, traffic on the exchange and clearing organization networks uses proprietary message protocols or formats, which are less vulnerable to the insertion of malicious messages or computer viruses. Although rendering the securities market networks generally less vulnerable, these features do not completely protect them and the prominence of securities market participants' role in the U.S. economy means that their networks are more likely to be targeted for electronic attack than some other sectors. The 15 organizations we reviewed in 2002 had generally implemented the elements of a sound information security program, including policies and procedures and access controls. Thirteen of the 15 organizations were also using intrusion detection systems, and the remaining 2 had plans to implement or were considering implementing such systems. All 15 of the organizations also had procedures that they would implement in the event of systems breaches, although the comprehensiveness of the incident response procedures varied. For example, 2 organizations' incident response plans

involved shutting down any breached systems, but lacked documented procedures for taking further actions such as gathering evidence on the source of the breach.

Developing business continuity capabilities is another way to reduce the risk of operations disruptions, and all 15 of the organizations we reviewed in 2002 had plans for continuing operations. These plans had a variety of contingency measures to facilitate the resumption of operations. For example, 11 organizations had backup facilities to which their staff could relocate if disruptions occurred at the primary facility. One of these organizations had three fully equipped and staffed facilities that could independently absorb all operations in an emergency or disruption. In some cases, organizations did not have backup facilities that could accommodate their operations but had taken steps to ensure that key business functions could be transferred to other organizations. For example, staff at one exchange that lacked a backup facility said that most of the products it traded were already traded on other exchanges, so trading of those products would continue if its primary site was not available. In addition, this exchange has had discussions with other exchanges about transferring trading of proprietary products to the other exchanges in an emergency situation. These organizations all had inventoried critical telecommunications and had made arrangements to ensure that they would continue to have service if primary lines were damaged.

**Some Financial
Organizations Had
Preparedness
Limitations That
Increased Their Risk of
an Operations
Disruption**

Although all 15 organizations we reviewed had taken steps to address physical and electronic threats and had BCPs to respond to disruptive events, but at the time of our review many had limitations in their preparedness that increased the risk of an operations disruption. Nine of the 15 organizations, including 2 critical organizations, were at greater risk of experiencing an operations disruption because their BCPs did not address how they would recover if a physical attack on their primary facility left a large percentage of their staff incapacitated. Although 5 of these 9 organizations had backup facilities, they did not maintain staff outside of their primary facility that could conduct all their critical operations. Eight of the 9 organizations also had physical security vulnerabilities at their primary sites that they either had not or could not mitigate. For example, these organizations were unable to control vehicular traffic around their facilities and thus were more exposed to damage than those that did have such controls.

Most of the organizations we reviewed also had faced increased risk that their operations would be disrupted by a wide-scale disaster. As of August 2002, all 7 of the critical organizations we reviewed had backup facilities, including 3 whose facilities were hundreds of miles from their primary facilities. For example, 1 organization had two data centers located about 500 miles apart, each capable of conducting the organization's full scope of operations in the event that one site failed. The organization also has a third site that can take over the processing needed for daily operations on a next-day basis. However, the backup facilities of the other four organizations were located 2 to 5 miles from their primary sites. If a wide-scale disaster caused damage or made a region greater than these distances inaccessible, these 4 organizations would be at greater risk for not being able to resume operations promptly.

Many of the other 8 organizations also had faced increased risk that their operations would be disrupted by wide-scale disasters. At the time we conducted our review, 2 of the 8 organizations had backup facilities that were hundreds of miles from their primary operations. The remaining 6 organizations faced increased risk of being disrupted by a wide-scale disaster because 4 lacked backup facilities, while 2 organizations had backup facilities that were located 4 to 10 miles from their primary operations facilities.⁵ Of the 4 organizations that lacked a backup facility, one had begun constructing a facility near its primary site.

Four of the organizations that lacked regionally dispersed backup facilities told us that they had begun efforts to become capable of conducting their operations at locations many miles from their current primary and backup sites. For example, NYSE has announced that it is exploring the possibility of creating a second active trading floor some miles from its current location. In contrast to the backup trading location NYSE built in the months following the attack, which would only be active should its current primary facility become unusable, the exchange plans to move the trading of some securities currently traded at its primary site to this new facility and have both sites active each trading day. However, if the primary site were damaged, the new site would be equipped to be capable of conducting all trading. In December 2002, NYSE staff told us that they were still evaluating the creation of this second active trading floor.

⁵In total, 4 of the 15 organizations had backup sites 5 miles or less from their primary sites.

For the organizations that lacked backup facilities, cost was the primary obstacle to establishing such capabilities. For example, staff at one organization told us that creating a backup location for its operations would cost about \$25 million, or as much as 25 percent of the organization's total annual revenue. Officials at the 3 organizations without backup sites noted that the products and services they provide to the markets are largely duplicated by other organizations, so their inability to operate would have minimal impact on the overall market's ability to function.

Although cost can be a limiting factor, financial market organizations have some options for creating backup locations that could be cost-effective. At least one of the organizations we reviewed has created the capability of conducting its trading operations at a site that is currently used for administrative functions. By having a dual-use facility, the organization has saved the cost of creating a completely separate backup facility. This option also would seem well suited to broker-dealers, banks, and other financial institutions because they frequently maintain customer service call centers that have large numbers of staff that could potentially be equipped with all or some of the systems and equipment needed for the firm's trading or clearing activities.

Some Financial Market
Organizations Not Fully
Testing Security Measures
or Business Continuity
Capabilities

Organizations can also minimize operations risk by testing their physical and information security measures and business continuity plans, but we found the 15 exchanges, clearing organizations, ECNs, and payment system processors were not fully testing all these areas. In the case of physical security, such assessments can include attempting to infiltrate a building or other key facility such as a data processing center or assessing the integrity of automated intrusion detection systems. In the case of information security, such assessments can involve attempts to access internal systems or data from outside the organization's network or by using software programs that identify, probe, and test systems for known vulnerabilities. For both physical and information security, these assessments can be done by the organization's own staff, its internal auditors, or by outside organizations, such as security or consulting firms.

The extent to which the 15 exchanges, clearing organizations, ECNs, and payment system providers that we reviewed had tested their physical security measures varied. Only 3 of the 7 critical financial organizations routinely tested their physical security; the tests included efforts to gain unauthorized access to facilities or smuggle fake weapons into buildings.

None of the remaining 8 organizations routinely tested the physical security of their facilities.

To test their information security measures, all 7 of the critical organizations had assessed network and systems vulnerabilities. We considered an organization's assessment current if it had occurred within the 2 years prior to our visit, because system changes over time can create security weaknesses, and advances in hacking tools can create new means of penetrating systems.⁶ According to the assessments provided to us by the 7 critical organizations, all had performed vulnerability assessments of the information security controls they implemented over some of their key trading or clearing systems within the last 2 years. However, these tests were not usually done in these organizations' operating environment but instead were done on test systems or during nontrading hours. Seven of the remaining 8 organizations we reviewed also had not generally had vulnerability assessments of their key trading or clearing networks performed with the 2 years prior to our review. However, in the last 2 years, all 15 organizations had some form of vulnerability assessments performed for their corporate or administrative systems, which they use to manage their organization or operate their informational Web sites.

Most of the 7 organizations critical to overall market functioning were conducting regular tests of their business continuity capabilities. Based on our review, 5 of the 7 critical organizations had conducted tests of all systems and procedures critical to business continuity. However, these tests were not usually done in these organizations' real-time environments. Staff at one organization told us that they have not recently conducted live trading from their backup site because of the risks, expense, and difficulty involved. Instead, some tested their capabilities by switching over to alternate facilities for operations simulations on nontrading days. One organization tested all components critical to their operations separately and over time, but it had not tested all aspects simultaneously. Of the 8 other financial market organizations we reviewed, only 2 had conducted regular BCP tests. One organization, however, had an extensive disaster recovery testing regimen that involved using three different scenarios: simulating a disaster at the primary site and running its systems and network from the backup site; simulating a disaster at the backup site and running the systems and network from the primary site; and running its

⁶We conducted our reviews at the premises of these organizations from February to June 2002.

systems and network from the consoles at the backup site with no staff in the control room at the primary site.

Organizations also discovered the benefits of conducting such tests. For example, because of lessons learned through testing, one organization learned vital information about the capabilities of third-party applications, identified the need to configure certain in-house applications to work at the recovery site, installed needed peripheral equipment at the backup site, placed technical documentation regarding third-party application installation procedures at the backup site, and increased instruction on how to get to the backup site if normal transportation routes were unavailable. An official at this organization told us that with every test, they expected to learn something about the performance of their BCP and identify ways to improve it.

Observations

The exchanges, clearing organizations, ECNs, and payment system providers that we reviewed had all taken various steps to reduce the risk that their operations would be disrupted by physical or electronic attacks. In general, the organizations we considered more critical to the overall ability of the markets to function had implemented the most comprehensive physical and information security measures and BCPs. However, limitations in some organizations' preparedness appeared to increase the risks that their operations could be disrupted because they had physical security vulnerabilities not mitigated with business continuity capabilities. The extent to which these organizations had also reduced the risk posed by a wide-scale disruption also varied. Because the importance of these organizations' operations to the overall markets varies, regulators are faced with the challenge of determining the extent to which these organizations should take additional actions to address these limitations to reduce risks to the overall markets.

Financial Market Regulators Lack Recovery Goals for Trading and Could Strengthen Their Operations Risk Oversight

Although banking and securities regulators have begun to take steps to prevent future disasters from causing widespread payment defaults, they have not taken important actions that would better ensure that trading in critical U.S. financial markets could resume smoothly and in a timely manner after a major disaster. The three regulators for major market participants, the Federal Reserve, OCC, and SEC are working jointly with market participants to develop recovery goals and sound business continuity practices that will apply to a limited number of financial market organizations to ensure that these entities can clear and settle transactions and meet their financial obligations after future disasters. However, the regulators' recovery goals and sound practices do not extend to organizations' trading activities or to the stock exchanges. The regulators also had not developed complete strategies that identify where trading could be resumed or which organizations would have to be ready to conduct trading if a major exchange or multiple broker-dealers were unlikely to be operational for an extended period. Individually, these three regulators have overseen operations risks in the past. SEC has a program—the Automation Review Policy (ARP)—for reviewing exchanges and clearing organizations efforts to reduce operations risks, but this program faces several limitations. Compliance with the program is voluntary, and some organizations have not always implemented important ARP recommendations. In addition, market participants raised concerns over the inexperience and insufficient technical expertise of SEC staff, and the resources committed to the program limit the frequency of examinations. Lacking specific requirements in the securities laws, SEC has not generally examined operations risk measures in place at broker-dealers. The Federal Reserve and OCC are tasked with overseeing the safety and soundness of banks' operations and had issued and were updating guidance that covered information system security and business continuity planning. They also reported annually examining information security and business continuity at the entities they oversee, but these reviews did not generally assess banks' measures against physical attacks.

Regulators Are Developing Recovery Goals and Sound Business Continuity Practices for Clearing Functions but Not for Trading Activities

Treasury and the financial regulators have various initiatives under way to improve the financial markets' ability to respond to future crises (we discuss these in app. II) and assess how well the critical assets of the financial sector are being protected.¹ As part of these initiatives, certain financial market regulators have begun to identify business continuity goals for the clearing and settling organizations for government and corporate securities.² On August 30, 2002, the Federal Reserve, OCC, SEC, and the New York State Banking Department issued the *Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*.³ The paper presents sound practices to better ensure that clearance and settlement organizations will be able to resume operations promptly after a wide-scale, regional disruption.⁴ The paper proposes these organizations adopt certain practices such as

- identifying the activities they perform that support these critical markets;
- developing plans to recover these activities on the same business day; and

¹As part of national efforts to address critical infrastructure protection, an interagency group of financial regulators was formed in October 2001. This group—the Financial and Banking Information Infrastructure Committee—includes SEC, the five depository institution regulators, and the regulators for futures, insurance, and government-sponsored enterprises. The group began efforts to identify critical assets in the financial sector, improve communication among regulators, and ensure that financial market organizations receive appropriate priority in telecommunications restoration. We discuss these efforts in more detail in appendix II of this report. A more complete description of the United States' efforts to ensure that its critical infrastructure is protected and how the financial sector has been included is contained in our report *Critical Infrastructure Protection: Efforts of Financial Services Sector to Address Cyber Threats*, GAO-03-173 (Washington, D.C.: Jan. 30, 2003).

²These markets include those for federal funds, foreign currencies, commercial paper, government securities, stocks, and mortgage-backed securities.

³Board of Governors of the Federal Reserve, OCC, and SEC, *Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (Washington, D.C.: Aug. 30, 2002). The New York State Banking Department also contributed to this paper and issued it separately.

⁴A wide-scale, regional disruption is one that causes a severe disruption of transportation, telecommunications, power, or other critical infrastructure components across a metropolitan or other geographic area and its adjacent communities that are economically integrated with it.

- having out-of-region resources sufficient to recover these operations that are not dependent on the same labor pool or transportation, telecommunications, water, and power.

The regulators plan to apply the sound practices to a limited number of financial market organizations whose inability to perform certain critical functions could result in a systemic crisis that threatens the stability of the financial markets. If these organizations were unable to sufficiently recover and meet their financial obligations, other market participants could similarly default on their obligations and create liquidity or credit problems. According to the white paper, the sound practices apply to “core clearing and settlement organizations,” which include market utilities that clear and settle transactions on behalf of market participants and the two clearing banks in the government securities market.⁵ In addition, the regulators expect firms that play significant roles in these critical financial markets also to comply with sound practices that are somewhat less rigorous. The white paper indicates that probably 15 to 20 banks and 5 to 10 broker-dealers have volume or value of activity in these markets sufficient to present a systemic risk if they were unable to recover their clearing functions and settle all their transactions by the end of the business day.

The regulators also sought comment on the appropriate scope and application of the white paper, including whether they should address the duration of disruption that should be planned for, the geographic concentration of backup sites, and the minimum distance between primary and backup facilities. After considering the comments they receive, the regulators intend to issue a final version in 2003 of the white paper that will present the practices to be adopted by clearance and settlement organizations for these markets.

Based on our analysis of the comment letters that have been sent to the regulators as of December 2002, market participants and other commenters have raised concerns over the feasibility and cost of the practices advocated by the white paper. The organizations that have commented on the paper include banks, broker-dealers, industry

⁵In addition to the effort to develop sound practices for the organizations involved in clearing, the Federal Reserve and SEC issued a paper that discusses and seeks comment on several potential alternatives for conducting clearing services in these markets. See Board of Governors of the Federal Reserve and SEC, *Interagency White Paper on Structural Change in the Settlement of Government Securities: Issues and Options* (Washington, D.C.: Aug. 30, 2002).

associations, information technology companies and consultants, and many of these organizations complimented the regulators for focusing attention on a critical area. However, many commenters have urged the regulators to ensure that any practices issued balance the cost of implementing improved business continuity capabilities against the likelihood of various types of disruptions occurring. For example, a joint letter from seven broker-dealers and banks stated that requiring organizations to make costly changes to meet remote possibilities is not practical. Other commenters urged regulators not to mandate minimum distances between primary sites and backup locations for several reasons. For example, some commenters noted that beyond certain distances, firms cannot simultaneously process data at both locations, which the regulators acknowledged could be between 60 to 100 kilometers. Rather than specify a minimum distance, others stated that the practices should provide criteria that firms should consider in determining where to locate their backup facilities. One broker-dealer commented that it had chosen the locations of its two operating sites to minimize the likelihood that both would be affected by the same disaster or disruption. It noted that its two sites were served by separate water treatment plants and power grids and different telecommunication facilities support each. A third commonly cited concern was that the regulators should implement the practices as guidelines, rather than rules. For example, one industry association stated, "Regulators should not impose prescriptive requirements, unless absolutely necessary, in order to enhance the firms' ability to remain competitive in the global market."

Ensuring that organizations recover their clearing functions would help ensure that settlement failures do not create a broader financial crisis, but regulators have not begun a similar effort to develop recovery goals and business continuity practices to ensure that trading activities can resume promptly in various financial markets. Trading activities are important to the U.S. economy because they facilitate many important economic functions, including providing means to productively invest savings and allowing businesses to fund operations. The securities markets also allow companies to raise capital for new ventures. Ensuring that trading activities resume in a smooth and timely manner would appear to be a regulatory goal for SEC, which is specifically charged with maintaining fair and orderly markets. However, Treasury and SEC staff told us that the white paper practices would be applied to clearing functions because such activities are concentrated in single entities for some markets or in very few organizations for others, and thus pose a greater potential for disruption. In contrast, they did not include trading activities or

organizations that conduct only trading functions, such as the securities exchanges, because these activities are performed by many organizations that could substitute for each other. For example, SEC staff said that if one of the exchanges was unable to operate, other exchanges or the ECNs could trade their products. Similarly, they said that individual broker-dealers are not critical to the markets because others firms can perform their roles.

Although regulators have begun to determine which organizations are critical for accomplishing clearing functions, identifying the organizations that would have to be ready for trading in U.S. financial markets to resume within a given period of time is also important. If key market participants are not identified and do not adopt sound business continuity practices, the markets may not have sufficient liquidity for fair and orderly trading. For example, in the past when NYSE experienced operations disruptions, the regional exchanges usually have also chosen to suspend trading until NYSE could resume. SEC staff have also previously told us that the regional exchanges may not have sufficient processing capacity to process the full volume usually traded on NYSE. If the primary exchanges are not operational, trading could be transferred to the ECNs, but regulators have not assessed whether such organizations have sufficient capacity to conduct such trading or whether other operational issues would hinder such trading.

SEC has begun efforts to develop a strategy for resuming stock trading for some exchanges, but the plan is not yet complete and does not address all exchanges and all securities. To provide some assurance that stock trading could resume if either NYSE or NASDAQ was unable to operate after a disaster, SEC has asked these exchanges to take steps to ensure their information systems can conduct transactions in the securities that the other organization normally trades. SEC staff told us each organization will have to ensure that its systems can properly process the varying number of characters in the symbols that each uses to represent securities. However, as of December 2002, SEC had not identified the specific capabilities that the exchanges should implement. For example, NASDAQ staff said that various alternatives are being proposed for conducting this trading and each would involve varying amounts of system changes or processing capacity considerations. In addition, although each exchange trades thousands of securities, NYSE staff told us that they are proposing to accommodate only the top 250 securities, and the remainder of NASDAQ's securities, which have smaller trading volumes, would have to be traded by the ECNs or other markets. NASDAQ staff said they planned to trade all

NYSE securities if necessary. NYSE staff also said that their members have been asked to ensure that the systems used to route orders to NYSE be ready to accept NASDAQ securities by June 2003. Furthermore, although some testing is under way, neither exchange has completely tested its ability to trade the other's securities. Strategies for other exchanges and products also have not been developed.

As noted in chapter 2 of this report, trading was not resumed in U.S. stock and options markets after the attacks until several key broker-dealers were able to sufficiently recover their operations. Resuming operations after disruptions can be challenging because large broker-dealers' trading operations can require thousands of staff and telecommunications lines. In some cases, organizations that may not appear critical to the markets in ordinary circumstances could become so if a disaster affects other participants more severely. For example, in the days following the attacks, one of the IDBs that previously had not been one of the most active firms was one of the few firms able to resume trading promptly.

Program, Staff, and Resource Issues Hamper SEC Oversight of Market Participants' Operations Risks

Lacking specific requirements under the securities laws, SEC uses a voluntary program to oversee exchange, clearing organization, and ECN information systems operations. U.S. securities laws, rules, and regulations primarily seek to ensure that investors are protected. For example, securities laws require that companies issuing securities disclose material financial information, and SRO rules require broker-dealers to determine the suitability of products before recommending them to their customers. The regulations did not generally contain specific requirements applicable to physical or information system security measures or business continuity capabilities. However, as part of its charge to ensure fair and orderly markets and to address information system and operational problems experienced by some markets during the 1980s, SEC created a voluntary program—ARP—that covered information technology issues at the exchanges, clearing organizations and, eventually, ECNs.⁶ SEC's 1989 ARP statement called for the exchanges and clearing organizations to establish

⁶Initially applied only to exchanges and clearing organizations, SEC extended these ARP guidance expectations under a rule issued in 1998 to any ECN that accounted for more than 20 percent of the trading volume of a particular security; as of September 2002, SEC staff reported that 10 ECNs were subject to all the ARP expectations. Other ECNs must comply with a varying number of the ARP expectations, such as submitting systems change notifications to SEC, depending on their trading volume.

comprehensive planning and assessment programs to test system capacities, develop contingency protocols and backup facilities, periodically assess the vulnerability of their information systems to external or internal threats, and report the results to SEC. SEC issued an additional ARP statement in 1991 that called for exchanges and clearing organizations to obtain independent reviews—done by external organizations or internal auditors—of their general controls in several information system areas.

**SEC ARP Reviews Address
Some Operations Risks but
Some Key
Recommendations Not
Addressed**

SEC's ARP staff conducted examinations of exchanges, clearing organizations, and ECNs that addressed their information security and business continuity. The examinations are based on ARP policy statements that cover information system security, business continuity planning, and physical security at data and information systems centers, but do not address how organizations should protect their entire operations from physical attacks. SEC's ARP program staff explained that they analyze the risks faced by each organization to determine which are the most important to review. As a result, the staff is not expected to review every issue specific to the information systems or operations of each exchange, clearing organization, and ECN during each examination. We found that SEC ARP staff were reviewing important operations risks at the organizations they examined. Based on our review of the 10 most recent ARP examinations completed between January 2001 and July 2002, 9 covered information system security policies and procedures, and 7 examinations covered business continuity planning.⁷ Only one examination—done after the September 11, 2001, attacks—included descriptions of the overall physical security improvements. SEC ARP staff told us that telecommunications resiliency was a part of normal examinations, but none of the examination reports we reviewed specifically discussed these organizations' business continuity measures for ensuring that their telecommunications services would be available after disasters. However, ARP staff said that all of these operations risk issues would be addressed as part of future reviews.

Although SEC's voluntary ARP program provides some assurance that securities markets are being operated soundly, some of the organizations subject to ARP have not taken action on some important

⁷The 10 examinations covered 9 organizations reviewed once and an organization reviewed twice during this period.

recommendations. Since its inception, ARP program staff recommendations have prompted numerous improvements in the operations of exchanges, clearing organizations, and ECNs. ARP staff also reviewed exchange and clearing organization readiness for the Year 2000 date change and decimal trading, and market participants implemented both industrywide initiatives successfully. However, because the ARP program was not implemented under SEC's rulemaking authority, compliance with the ARP guidance is voluntary. Although SEC staff said that they were satisfied with the cooperation they received from the organizations covered by the ARP program, in some cases, organizations did not take actions to correct significant weaknesses ARP staff identified.⁸ For example, as we reported in 2001, three organizations had not established backup facilities, which SEC ARP staff had raised as significant weaknesses. Our report noted, "Securities trading in the United States could be severely limited if a terrorist attack or a natural disaster damaged one of these exchange's trading floor." In addition, for years, SEC's ARP staff raised concerns and made recommendations relating to inadequacies in NASDAQ's capacity planning efforts, and NASDAQ's weaknesses in this area delayed the entire industry's transition to decimal pricing for several months.⁹ NASDAQ staff told us they have implemented systems with sufficient capacity, and SEC staff said they are continuing to monitor the performance of these systems. We also reported that exchanges and clearing organizations sometimes failed to submit notifications to SEC regarding systems changes and outages as expected under the ARP policy statement, and we again saw this issue being cited in 2 of 10 recent ARP examination reports we reviewed.

ARP staff continue to find significant operational weaknesses at the organizations they oversee. In the 10 examinations we reviewed, SEC staff found weaknesses at all 9 organizations and made 74 recommendations for improvement. We compared these weaknesses to the operational elements we used in our analysis of financial market organizations (as discussed in ch. 3 of this report).¹⁰ Our analysis showed that the ARP staff made at least 22 recommendations to address significant weaknesses in the 9 organizations' physical or information system security or business

⁸U.S. General Accounting Office, *Information Systems: Opportunities Exist to Strengthen SEC's Oversight of Capacity and Security*, GAO-01-863 (Washington, D.C.: Jul. 25, 2001).

⁹See U.S. General Accounting Office, *Securities Pricing: Trading Volumes and NASD System Limitations Led to Decimal-Trading Delay*, GGD/AIMD-00-319 (Washington, D.C.: Sept. 20, 2000).

continuity planning efforts—including 10 recommendations to address significant weaknesses at organizations critical to the functioning of the markets. For example, in an examination conducted in 2000, ARP staff found that personnel at one exchange did not have consistent information system security practices across the organization and lacked a centrally administered, consolidated information system security policy.¹¹ In addition, although SEC recommends that organizations subject to ARP have vulnerability assessments performed on their information systems, ARP staff found that this exchange had not assessed its information systems. In three other reviews, the ARP staff found that the organizations had not complied with ARP policy expectations to fully test their contingency plans. ARP staff noted other significant weaknesses, including inadequate BCPs or backup facilities. ARP staff said that they considered all the recommendations they make to be significant, including the 74 recommendations made in these 10 reports. These recommendations will remain open until the next time the ARP staff review the organization and can assess whether they have been acted upon.

Because the ARP program was established through a policy statement and compliance is voluntary, SEC lacks specific rules that it can use to gain improved responsiveness to recommendations to the exchanges and clearing organizations subject to APP. SEC staff explained that they chose not to use a rule to implement ARP because rules can become obsolete and having voluntary guidance provides them with flexibility. SEC staff also told us that an organization's failure to follow ARP expectations could represent a violation of the general requirement that exchanges maintain the ability to operate, and therefore they could take action under that authority. However, they noted that the use of such authority is rare. However, SEC has issued a rule requiring the most active ECNs to comply with all the ARP program's standards. In 1998, SEC issued a regulation that subjected alternative trading systems such as ECNs to increased regulatory scrutiny because of their increasing importance to U.S. securities markets. Included in this regulation was a rule that required ECNs whose trading volumes exceeded certain thresholds to comply with the same practices as

¹⁰For our analysis, we classified the weaknesses that SEC identified as significant when the organization had not implemented adequate procedures or capabilities in the key elements we used to evaluate the 15 organizations included in this report, as discussed in chapter 3.

¹¹This exchange was not among the organizations we considered critical to the functioning of the markets in our analysis.

those contained in the ARP policy statements.¹² In its explanation of the regulation, SEC noted that its ARP guidelines are intended to ensure that short-term cost cutting by registered exchanges does not jeopardize the operation of the securities markets, and therefore it was extending these requirements to the ECNs because of their potential to disrupt the securities markets.

We previously recommended that SEC develop formal criteria for assessing exchange and clearing organization cooperation with the ARP program and perform an assessment to determine whether the voluntary status of the ARP program is appropriate.¹³ Although they were generally satisfied with the level of cooperation, SEC staff told us that they were reviewing the extent to which exchanges and clearing organizations complied with the ARP program and planned to submit the analysis to SEC commissioners in 2003. In addition to possibly changing the status of the program for the 22 exchanges and clearing organizations subject to ARP, SEC staff also told us that they were considering the need to extend the ARP program to those broker-dealers for whom it would be appropriate to adopt the sound business continuity practices that will result from the joint regulatory white paper.

SEC ARP Program Faces Resource and Staff Limitations

Limited resources and challenges in retaining experienced ARP staff have affected SEC's ability to oversee an increasing number of organizations and more technically complex market operations. Along with industrywide initiatives discussed earlier, ARP staff workload has expanded to cover 32 organizations with more complex technology and communications networks. However, SEC has problems retaining qualified staff, and market participants have raised concerns about the experience and expertise of ARP staff. As SEC has experienced considerable staff losses overall, the ARP program also has had high turnover. As of October 2002, ARP had 10 staff, but SEC staff told us that staff levels had fluctuated and had been as low as 4 in some years.¹⁴ As a result, some ARP program staff had limited experience, with 4 of the 10 current staff having less than 3.5 years' experience, including 3 with less than 2 years' experience. During our work on SEC resource issues in 2001, market participants and former SEC staff

¹²SEC, *Regulation of Exchanges and Alternative Trading Systems: Final Rules*, Release No. 34-40760 (Dec. 8 1998).

¹³[GAO-01-863](#).

¹⁴[GAO-01-863](#).

raised concerns that the level of resources and staff expertise SEC has committed to review technology issues is inadequate to address complex market participant operations.¹⁵ For example, officials from several market participants we interviewed in 2001 told us that high turnover resulted in inexperienced SEC staff, who lacked in-depth knowledge, doing reviews of their organizations. SEC staff told us that they continue to emphasize training for their staff to ensure that they have the proper expertise to conduct effective reviews.

Resource limitations also affect the frequency of ARP reviews. With current staffing levels, SEC staff said that they are able to conduct examinations of only about 7 of the 32 organizations they oversee as part of the ARP program each year.¹⁶ Although standards for federal organizations' information systems require security reviews to be performed at least once every 3 years, these standards recommend that reviews of high-risk systems or those undergoing significant systems modifications be done more frequently.¹⁷ Although our analysis of SEC ARP examination data found that SEC had conducted recent reviews of almost all the organizations we considered critical to the financial markets, long periods of time often elapsed between ARP examinations of these organizations.¹⁸ Between September 1999 and September 2002, SEC examined 6 of the 7 critical organizations under its purview.¹⁹ However, as shown in figure 12, the intervals between the most recent examinations exceeded 3 years for 5

¹⁵U.S. General Accounting Office, *SEC Operations: Increased Workload Creates Challenges*, GAO-02-302 (Washington, D.C.: Mar. 5, 2002).

¹⁶In addition to examinations, the SEC ARP staff also monitor the organizations subject to ARP by conducting a risk analysis of each organization each year, reviewing internal and external audits performed of these organizations' systems, and receiving notices of systems changes and systems outages from these organizations.

¹⁷Office of Management and Budget, *Appendix III to OMB Circular A-130: Security of Federal Automated Information Resources*.

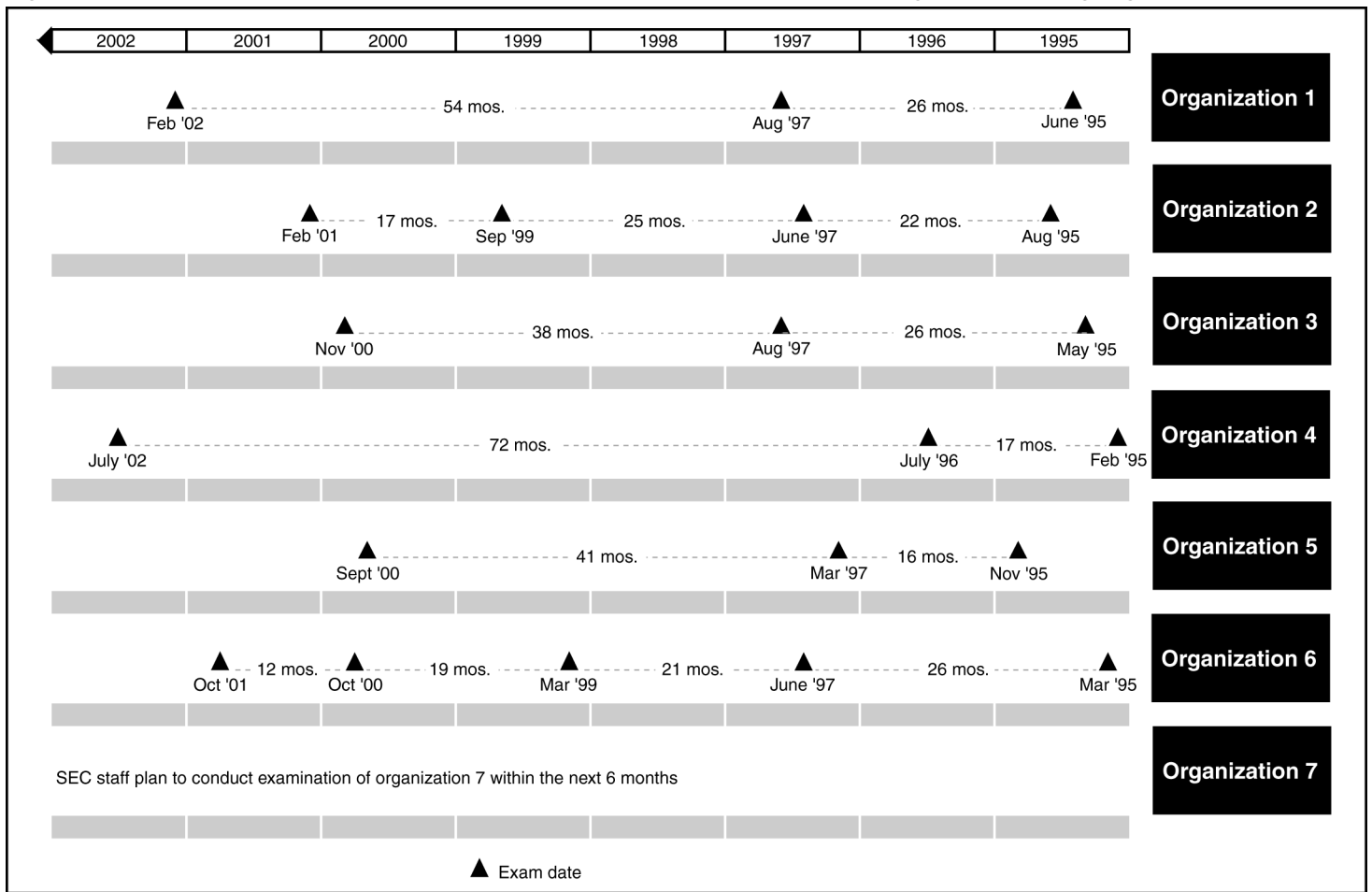
¹⁸Of the 7 organizations that we considered critical to the overall functioning of the markets for purposes of chapter 3, 5 are subject to the ARP program. Because of the way they are organized, these 5 organizations actually are 7 distinct entities that the SEC ARP staff reviews separately. SEC staff agreed that these organizations were important to the markets.

¹⁹SEC ARP staff told us that they had not reviewed one organization since 1994 because its operations, although critical to the markets, had not presented issues that warranted a high-risk designation. However, they said they planned to conduct a review of this organization within the next 6 months.

**Chapter 4
Financial Market Regulators Lack Recovery
Goals for Trading and Could Strengthen
Their Operations Risk Oversight**

of the 7 critical organizations, including an organization that was not reviewed during this period.

Figure 12: Intervals between Most Recent SEC ARP Examinations of Critical Exchanges and Clearing Organizations



Source: SEC.

Our analysis of ARP report data showed that the intervals between reviews of critical organizations averaged 39 months, with the shortest interval being 12 months and the longest 72 months. Since September 1999, the SEC ARP staff had reviewed 7 of the 8 less critical exchanges, clearing organizations, and ECNs that we visited during this review. However, SEC staff told us that the ARP program also may be tasked with reviewing the extent to which broker-dealers important to clearing and trading in U.S.

securities markets are adhering to sound business continuity practices. Such an expansion in the ARP program staff's workload would likely further reduce the ability of the SEC staff to frequently review all the important organizations under its authority.

Increased Appropriations Could Provide SEC an Opportunity to Improve ARP Program Resources

The potential increase in SEC's appropriations could provide the agency an opportunity to increase the level and quality of the resources it has committed to the ARP program. The Sarbanes-Oxley Act of 2002, which mandated various accounting reforms, also authorized increased appropriations for SEC for fiscal year 2003.²⁰ Specifically, the act authorized \$776 million in 2003, an increase of about 51 percent over the nearly \$514 million SEC received for fiscal year 2002.²¹ The act directs SEC to devote \$103 million of the newly authorized amount to personnel and \$108 million to information technology. If appropriated, these additional funds could allow SEC to increase resources devoted to the ARP program. Increased staffing levels also could allow SEC to conduct more frequent examinations and better ensure that significant weaknesses are identified and addressed in a timely manner. The additional resources could also be used to increase the technical expertise of its staff, further enhancing SEC's ability to review complex information technology issues.

SEC and SROs Generally Did Not Review Physical and Information System Security and Business Continuity at Broker-Dealers

SEC and the securities market SROs generally have not examined broker-dealers' physical and information system security and business continuity efforts, but planned to increase their focus on these issues in the future. SEC's Office of Compliance Inspections and Examinations (OCIE) examines broker-dealers, mutual funds, and other securities market participants.²² However, for the most part, OCIE examinations focus on broker-dealers' compliance with the securities laws and not on physical and electronic security and business continuity, which these laws do not generally address. After some broker-dealers that specialized in on-line trading experienced systems outages, OCIE staff told us that they began addressing information system capacity, security, and contingency capabilities at these firms. SEC predicated its reviews of these issues on

²⁰Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002).

²¹This \$514 million includes an original appropriation of \$438 million, a \$21 million supplemental appropriation for September 11-related disaster recovery, \$25 million to implement pay parity, and over \$30 million in additional supplemental appropriations.

²² SEC also oversees investment advisers and transfer agents.

the fact that these firms, as a condition of conducting a securities business, would need to have sufficient operational capacity to enter, execute, and settle orders, and deliver funds and securities promptly and accurately. In addition, the Gramm-Leach-Bliley Act (GLBA) required SEC to establish standards for the entities it oversees to safeguard the privacy and integrity of customer information and prevent unauthorized disclosure.²³ As a result, in some reviews done since July 2001, OCIE staff discussed the controls and policies that firms have implemented to protect customer information from unauthorized access. However, SEC OCIE staff acknowledged that their expertise in these areas is limited. OCIE staff told us that few of the approximately 600 examiners they employ had information technology backgrounds. During the work we conducted for our report on SEC's staffing and workload, staff at several broker-dealers told us that the SEC staff that review their firms lacked adequate technology expertise.²⁴

SROs also generally have not addressed these issues at broker-dealers. Under U.S. securities laws, exchanges acting as SROs have direct responsibility for overseeing their broker-dealer members. NYSE and NASD together oversee the majority of broker-dealers in the United States.²⁵ According to officials at these two SROs, staff as often as annually conduct examinations to review adherence with capital requirements and other securities regulations. However, staff at both organizations acknowledged that, in the past, their oversight generally did not focus on how members conducted their operations from physical or information systems security or business continuity perspectives. Representatives of the SROs told us they plan to include aspects of these issues in future reviews. For example, they plan to examine their members' information system security to ensure compliance with GLBA customer information protection provisions.

NYSE and NASD plan to focus on business continuity issues in future reviews because, in August 2002, both submitted similar rules for SEC approval that will require all of their members to establish BCPs. The areas the plans are to address include the following:

²³15 U.S.C. §§ 6801, 6805.

²⁴GAO-02-302.

²⁵The other stock and options exchanges and clearing organizations also have self-regulatory responsibilities over their members, but generally are only directly responsible for examining those members not already overseen by another SRO.

- backup for books and records,
- procedures for resuming operations of critical systems,
- alternate means for communicating with the members' staff and their customers, and
- regulatory reporting and communications with regulators.

NYSE and NASD officials told us that once these rules were adopted, their staff would include these matters in the scope of their examinations after allowing sufficient time for firms to develop the required BCPs.

Bank Regulators Have Authority to Oversee Operational Risk

As part of their mandate to oversee banks' safety and soundness, the banking regulators, including the Federal Reserve and OCC, issued guidance that directs depository institutions or banks to address potential operations risks with physical and information system security and business continuity measures. The guidance includes recommended steps that banks should take to reduce the risk of operations disruptions from physical or electronic attacks and for recovering from such events with business continuity capabilities. For example, in 1996 these regulators jointly issued a handbook on information systems, which calls for banks to conduct an analysis of their risks and implement measures to reduce them.²⁶ Banks were also to have access controls for their systems and programs. Regarding physical security, the banking regulators expect banks to ensure the safety of assets and to physically protect data centers used for information systems processing. For example, the Federal Reserve's guidance directs banks to take security steps to protect cash and vaults and ensure that bank facilities are protected from theft. The banking regulators' joint 1996 handbook discussed measures to secure data centers and information system assets. However, the bank regulators' guidance did not specifically address measures to protect facilities from terrorist or other physical attacks. Regarding business continuity, the joint handbook expects banks to have plans addressing all critical services and operations necessary to minimize disruptions in service and financial losses and ensure timely resumption of operations in a disaster. Banks also were to identify the critical components of their telecommunications networks and

²⁶Federal Financial Institutions Examination Council, *Information Systems Examination Handbook, Vol. 1* (Washington, D.C.: 1996).

assess whether they were subject to single points of failure that could occur, for example, by having all lines routed to a single central switching office, and to identify alternate routes and implement redundancy.

The Federal Reserve and OCC, in conjunction with the other depository regulators, are also developing expanded guidance on physical and electronic security and business continuity planning. They are planning to issue separate handbooks on information system security and business continuity in early 2003. Bank regulatory staff provided us with a draft of the information system security guidance, which expects banks to have programs that include security policies, access controls, and intrusion monitoring; vulnerability assessments; and incident response capabilities. The draft guidance also covers physical security from an overall facility perspective and suggests that banks use appropriate controls to restrict or prevent unauthorized access and prevent damage from environmental contaminants. Banks will also be instructed to assess their exposure risks for fire and water damage, explosives, or other threats arising from location, building configuration, or neighboring entities. According to bank regulatory staff, they are also currently drafting a separate guidance handbook addressing business continuity issues.

**Bank Regulators Reported
Reviewing Operations Risks
but Not Banks' Measures
Against Physical Attacks**

Bank regulators reported regularly examining how banks are addressing physical and information system security and business continuity issues. The Federal Reserve and OCC oversee over 3,100 institutions combined, including the largest U.S. banks, and are required to examine most institutions annually. At the end of fiscal year 2002, the Federal Reserve had over 1,200 examiners and OCC over 1,700. As part of these staff, the agencies each had between 70 and 110 examiners that specialized in reviewing information systems issues. Using a risk-based approach, these regulators' examiners tailor their examinations to the institution's unique risk profile. As a result, some areas would receive attention every year, but others would be examined only periodically. Staff at the Federal Reserve and OCC told us that their examiners consider how their institutions are managing operations risks and review these when appropriate. For example, Federal Reserve staff told us that under their risk-based examination approach, information security is considered as part of each examination, particularly since regulations implementing section 501(b) of GLBA require that the regulators assess how financial institutions protect customer information. They said that the extent to which information security is reviewed at each institution can vary, with less detailed reviews generally done at institutions not heavily reliant on information technology.

They also said that business recovery issues were addressed in most examinations. Both Federal Reserve and OCC staff told us that physical security was considered as part of information security in reviewing protections at data centers. Both regulators also expect banks' internal auditors to review physical security for vault and facilities protection. However, the focus of these reviews has not generally been on the extent to which banks are protected from terrorist or other physical attacks. In light of the September 2001 attacks, these regulators stated that their scrutiny of physical and information system security and business continuity policies and procedures would be reviewed even more extensively in future examinations. Because we did not review bank examinations as part of our review, we were unable to independently determine how often and how extensively these two bank regulatory agencies reviewed information security and business continuity at the entities they oversee.

Conclusions

Financial market regulators have begun to develop goals and a strategy for resuming operations along with sound business continuity practices for a limited number of organizations that conduct clearing functions. The business continuity practices that result from this effort will likely address several important areas, including geographic separation between primary and backup locations and the need to ensure that organizations have provisions for separate staff and telecommunications services needed to conduct critical operations at backup locations. If successfully implemented, these sound practices should better ensure that clearing in critical U.S. financial markets could resume and settlement would be completed after a disaster, potentially avoiding a harmful systemic crisis.

However, trading on the markets for corporate securities, government securities, and money market instruments is also vitally important to the economy, and the United States deserves similar assurance that trading activities would also be able to resume when appropriate and without excessive delay. The U.S. economy has demonstrated that it can withstand short periods during which markets are not trading. After some events occur, having markets closed for some time could be appropriate to allow for disaster recovery and reduce market overreaction. However, long delays in reopening the markets could also be harmful to the economy. Without trading, investors lack the ability to accurately value their securities and would be unable to adjust their holdings. The attacks demonstrated that the ability of markets to recover could depend on the extent to which market participants have made sound investments in business continuity capabilities. Without identifying strategies for recovery,

determining the sound practices needed to implement these strategies, and identifying the organizations that would conduct trading under these strategies, the risk that markets may not be able to resume trading in a fair and orderly fashion and without excessive delays is increased. Goals and strategies for recovering trading activities could be based on likely disaster scenarios that identify the organizations that could be used to conduct trading in the event that other organizations were unable to recover within a reasonable time. These would provide market participants with information to make better decisions about how to improve their operations and provide regulators with sound criteria for ensuring that trading on U.S. markets could resume when appropriate.

Strategies for resuming trading could involve identifying which markets would assume the trading activities of others or identifying other venues such as ECNs in which trading could occur. To be viable, these strategies would also have to identify whether any operational changes at these organizations would be necessary to allow this trading to occur. Although SEC has begun efforts to ensure that trading can be transferred between NYSE and NASDAQ, these efforts are not complete and not all securities are covered. Because of the risk of operational difficulties resulting from large-scale transfers of securities trading to organizations that normally do not conduct such activities, testing the various scenarios would likely reduce such problems and ensure that the envisioned strategies are viable.

Expanding the organizations that would be required to implement sound business continuity practices beyond those important for clearing would better ensure that those organizations needed for the resumption of smooth and timely trading would have developed the necessary business continuity capabilities. As discussed in chapter 3, exchanges, clearing organizations, and ECNs we reviewed had taken many steps to reduce the risks that they would be disrupted by physical or electronic attacks and have mitigated risk through business continuity planning. However, some organizations still had limitations in their business continuity measures that increased the risk that their operations would be disrupted, including organizations that might need to trade if the major exchanges were unable to resume operations. In addition, the attacks demonstrated that organizations that were not previously considered critical to the markets' functioning could greatly increase in importance following a disaster. Therefore, identifying all potential organizations that could become important to resuming trading and ensuring they implement sound business practices would increase the likelihood of U.S. financial markets being able to recover from future disasters. Given that the importance of

different organizations to the overall markets varies, any recovery goals and business continuity practices that are developed could similarly vary their expectations for different market participants but with the ultimate goal of better ensuring that organizations take reasonable, prudent steps in advance of any future disasters. For example, broker-dealers could be expected to take steps to ensure that their customer records are backed up frequently and that these backup records are maintained at considerable distance from the firms' primary sites. This would allow customers to transfer their accounts to other broker-dealers if the firm through which they usually conduct trading is not operational after a major disaster.

Given the increased threats demonstrated by the September 11 attacks and the need to ensure that key financial market organizations are following sound practices, securities and banking regulators' oversight programs are important mechanisms for ensuring that U.S. financial markets are resilient. However, SEC's ARP program—which oversees the key clearing organizations and exchanges and may be used to oversee additional organizations' adherence to the white paper on sound practices—currently faces several limitations. Because it is a voluntary program, SEC lacks leverage to assure that market participants implement important recommended improvements. An ARP program that draws its authority from an issued rule could provide SEC additional assurance that exchanges and clearing organizations adhere to important ARP recommendations and any new guidance developed jointly with other regulators. To preserve the flexibility that SEC staff see as a strength of the current ARP program, the rule would not have to mandate specific actions but could instead require that the exchanges and clearing organizations engage in activities consistent with the practices and tenets of the ARP policy statements. This would provide SEC staff with the ability to adjust their expectations for the organizations subject to ARP as technology and industry best practices evolve while providing clear regulatory authority to require prudent actions when necessary. SEC already requires ECNs to comply with ARP guidance; extending the rule to the exchanges and clearing organizations would place them on similar legal footing.

Additional staff, including those with technology backgrounds, could better ensure the effectiveness of the ARP program's oversight. SEC could conduct more frequent examinations, as envisioned by federal information technology standards, and more effectively review complex, large-scale technology operations in place at the exchanges, ECNs, and clearing organizations. If the ARP program must also begin reviewing the extent to which broker-dealers important to clearing and trading in U.S. securities

markets are adhering to sound business continuity practices, additional staff resources would likely be necessary to prevent further erosion in the ability of the SEC staff to oversee all the important organizations under its authority. The increased appropriations authorized in the Sarbanes-Oxley Act, if received, would present SEC a clear opportunity to enhance its technological resources, including the ARP program, without affecting other important initiatives.

Recommendations

So that trading in U.S. financial markets can resume after future disruptions in as timely a manner as appropriate, we recommend that the Chairman, SEC, work with industry to

- develop goals and strategies to resume trading in securities;
- determine sound business continuity practices that organizations would need to implement to meet these goals;
- identify the organizations, including broker-dealers, that would likely need to operate for the markets to resume trading and ensure that these entities implement sound business continuity practices that at a minimum allow investors to readily access their cash and securities; and
- test trading resumption strategies to better assure their success.

In addition, to improve the effectiveness of the SEC's ARP program and the preparedness of securities trading and clearing organizations for future disasters, we recommend that the Chairman, SEC, take the following actions:

- Issue a rule requiring that the exchanges and clearing organizations engage in activities consistent with the operational practices and other tenets of the ARP program; and
- If sufficient funding is available, expand the level of staffing and resources committed to the ARP program.

Agency Comments and Our Evaluation

We requested comments on a draft of this report from the heads, or their designees, of the Federal Reserve, OCC, Treasury, and SEC. The Federal Reserve and SEC provided written comments, which appear in appendixes

III and IV, respectively. The Federal Reserve, OCC, and SEC also provided technical comments, which we incorporated as appropriate.

SEC generally agreed with the report and the goals of its recommendations. The letter from SEC's Market Regulation Division Director noted that SEC has been working with market participants to strengthen their resiliency and that the SEC staff agreed that the financial markets should be prepared to resume trading in a timely, fair, and orderly fashion following a catastrophe, which is the goal of our recommendations that SEC work with the industry to develop business continuity goals, strategies, and practices. SEC's letter expressed a concern that this recommendation expects SEC to ensure that broker-dealers implement business continuity practices that would allow trading activities to resume after a disaster. The SEC staff noted that broker-dealers are not required to conduct trading or provide liquidity to markets. Instead this would be a business decision on the part of these firms. However, SEC's letter noted that broker-dealers are required to be able to ensure that any completed trades are cleared and settled and that customers have access to the funds and securities in their accounts as soon as is physically possible. SEC's letter stated that the BCP expectations for these firms must reflect these considerations.

We agree with SEC that the business continuity practices they develop with broker-dealers should reflect that the extent to which these firms' BCPs address trading activities is a business decision on the part of a firm's management. In addition, SEC would need to take into account the business continuity capabilities implemented by broker-dealers that normally provide significant order flow and liquidity to the markets when it works with the exchanges and other market participants to develop goals and strategies for recovering from various disaster scenarios. To the extent that many of these major broker-dealers may be unable to conduct their normal volume trading in the event of some potential disasters without extended delays, the intent of our recommendation is that SEC develop strategies that would allow U.S. securities markets to resume trading, when appropriate, through other broker-dealers such as regional firms that are less affected by the disaster. However, to ensure that such trading is orderly and fair to all investors, SEC will have to ensure that broker-dealers' business continuity measures at a minimum are adequate to allow prompt transfers of customer funds and securities to other firms so that the customers of firms unable to resume trading are not disadvantaged.

Regarding our recommendations to ensure that SEC's ARP program has sufficient legal authority and resources to be an effective oversight

Chapter 4
Financial Market Regulators Lack Recovery
Goals for Trading and Could Strengthen
Their Operations Risk Oversight

mechanism over exchanges, clearing organizations, and ECNs, SEC's Market Regulation Division Director stated that they will continue to assess whether rulemaking is appropriate. In addition, the letter stated that, if the agency receives additional funding, they will consider recommending to the Chairman that ARP staffing and resources be increased.

SEC's letter also commented that physical security beyond the protection of information technology resources was not envisioned as a component of ARP when the program was initiated. They indicated that they may need additional resources and expertise to broaden their examinations to include more on this issue.

In the letter from the Federal Reserve's Staff Director for Management, he noted that the Federal Reserve is working to improve the resilience of the financial system by cooperating with banking and securities regulators to develop sound practices to reduce the system effects of wide-scale disruptions. They are also working with the other banking regulators to expand the guidance for banks on information security and business continuity.

Telecommunications Providers and Others Cooperated to Overcome Damage to Telecommunications Infrastructure

The September 11 attacks caused extensive damage to telecommunications infrastructure and resulted in loss of telecommunications services to financial market participants in lower Manhattan. During the days that followed, the affected telecommunications carriers worked together with financial market participants and local government officials to overcome numerous challenges to restore key services and reestablish the connectivity needed to reopen the nation's equity markets on September 17, 2001.

The Terrorist Attacks Extensively Damaged Local Telecommunications Infrastructure

The September 11 terrorist attacks extensively damaged the telecommunications infrastructure serving lower Manhattan, disrupting voice and data communications services throughout the area. The bulk of this damage occurred when 7 World Trade Center collapsed into an adjacent building—a major Verizon telecommunications center at 140 West Street. Because the Verizon central office was the major local communications hub within the public network, the collateral damage to that facility significantly disrupted local telecommunications services to approximately 34,000 businesses and residences in the surrounding area, including the financial district.¹

Significant numbers of customers lost their telecommunications services for extended periods. When the Verizon central office was damaged, about 182,000 voice circuits, more than 1.6 million data circuits, almost 112,000 PBX trunks, and more than 11,000 lines serving Internet service providers were lost.² This central office served a large part of lower Manhattan. (The area served by this facility is shown in fig. 8 in ch. 2.)

The attacks also damaged other Verizon facilities and affected customers in areas beyond that served directly from 140 West Street. Three other Verizon switches in the World Trade Center towers and in 7 World Trade Center were also destroyed in the attacks. Additional services were disrupted

¹A central office is a telephone company facility containing the switching equipment that links served customers to the public voice and data networks within and outside of the local service area.

²A PBX (private branch exchange) is an automatic telephone switching system that is owned, operated, and located within a private enterprise. This system switches calls between enterprise users on local lines while allowing all users to share a certain number of external telephone lines. A PBX trunk line connects the PBX to the serving telecommunications carrier's local central office switch.

Appendix I
Telecommunications Providers and Others
Cooperated to Overcome Damage to
Telecommunications Infrastructure

because 140 West Street also served as a transfer station on the Verizon network for about 2.7 million circuits carrying data traffic that did not originate or terminate in that serving area, but that nevertheless passed through that physical location. For example, communications services provided out of the Verizon Broad Street central office that passed through West Street were also disrupted until new cabling could be put in place to physically carry those circuits around the damaged facility. As a result, Verizon had to restore services provided by about 4.4 million Verizon data circuits in total.

The attacks also damaged the facilities and equipment of other carriers as well. In the 140 West Street facilities, 30 other telecommunications providers had equipment linking their networks to the Verizon network. Allegiance Telecom, Covad Communications, Metromedia Fiber Network, PaeTec, XO Communications, and Winstar Communications noted the interdependence of network services and that the cascading effect of the Verizon network disruptions affected tens of thousands of their customers according to outage reports filed with the Federal Communications Commission (FCC). Other local carriers also sustained losses to their own network facilities. For example, AT&T Local Network Service lost use of two major network nodes in the World Trade Center complex, as well as two switches in damaged buildings. Service provided by two other switches were disrupted when the switches lost power. AT&T also lost use of the fiber-optic cable that provided its own local service to lower Manhattan. Overall, AT&T lost equipment and circuits including 200 miles of fiber-optic cable, more than 33 thousand network trunks, and about 20,000 other telecommunications lines that each carried the equivalent of 24 voice communication channels.³ Focal Communications reported to FCC that customers served by its switch in lower Manhattan lost service at about 11:00 p.m. on September 11, 2001, when commercial power to that switch was lost, and backup power supplies (generator, then battery) were eventually exhausted before Focal Communications technicians could gain access to their facilities in order to restore power.

After September 11, some financial firms whose physical facilities were not damaged learned that telecommunications services still could fail because their supporting services were not as diverse and redundant as expected. Diversity involves establishing different physical routes into and out of a

³A trunk is a telecommunications line that carries multiple voice or data channels between two telephone exchange switching systems.

Appendix I
Telecommunications Providers and Others
Cooperated to Overcome Damage to
Telecommunications Infrastructure

building, and using different equipment along those routes to prevent failures if a disaster or other form of interference adversely affects one route. Redundancy involves having extra capacity available, generally from more than one source, and also incorporates aspects of diversity. Therefore, users that rely on telecommunications services to support important applications try to ensure that those services use facilities that are diverse and redundant so that no single point in the communications path can cause all services to fail.

After the attacks, some firms that made arrangements with multiple service providers to obtain redundant service discovered that the lines used by their providers were not diverse because they routed through the same Verizon switching facility. Other firms that had mapped out their communications lines to ensure that their lines flowed through physically diverse paths at the time those services were first acquired found that their service providers had rerouted some of those lines over time without their knowledge, eliminating that assurance of diversity in the process. Representatives of several banks and broker-dealers with major New York operations told us that they suffered disruptions to their telecommunications service despite their belief that they were being served by diverse carriers, diverse facilities, or both.

Ensuring that carriers actually maintain physically redundant and diverse telecommunications services has been a long-standing concern within the financial industry. For example, in December 1997, the President's National Security Telecommunications Advisory Committee reported, "despite assurances about diverse networks from the carriers, a consistent concern among the financial services industry was the trustworthiness of their telecommunications diversity arrangements."⁴

Obtaining physically diverse telecommunications services and ensuring that diversity is maintained over time is difficult. First, some customers incorrectly assume that simply obtaining service from multiple carriers ensures that they are receiving redundant and diverse services. However, a competing local carrier may choose to lease or resell the "last mile" circuits into a customer location from the incumbent local exchange carrier rather

⁴The President's National Security Telecommunications Advisory Committee, *Financial Services Risk Assessment Report*, December 1997.

than incur the cost to construct its own facilities into a building.⁵ In New York City for example, providing facilities in a given building and constructing lines from network facilities running through an adjacent street can typically cost a carrier about \$150,000. This total does not include the time and cost associated with obtaining a building owner's permission to locate facilities on premise. Also, where multiple carriers have a network presence in a given property, different carrier circuits could possibly share the same rights-of-way and conduits to enter and exit a building. Moreover, as was learned in the aftermath of September 11, assurances regarding diversity also could lose validity as telecommunications carriers merge or change the paths of circuits over time.

Telecommunications Carriers and Government Agencies Worked Together to Overcome Challenges

Telecommunications carriers and government entities collaborated to restore telecommunications after the attacks. Before work could begin to restore the connections supporting the financial markets, telecommunications providers first had to ensure that government services, including public safety, and health care providers had service. Restoring service to all affected organizations required telecommunications providers to overcome significant challenges, including obtaining access to the affected area and working under hazardous conditions.

Telecommunications Carriers Gave First Priority to Government and Health Care Services

Although regulators and market participants were anxious to reopen the financial markets, the immediate priority for telecommunications carriers in the aftermath of the attacks was to restore service to the government and health care sectors in New York City. As required by federal emergency response protocols, telecommunications carriers' first priority was to ensure that critical services to city, state, and federal government entities were restored, in particular circuits that had been designated as Telecommunications Service Priority circuits because they supported communications relating to national security and emergency preparedness. Carriers provided new or rerouted communications lines to support public safety and other emergency services personnel in the affected area,

⁵The specific physical segment that connects each residential or business customer to the initial telephone company central office is referred to as the "local loop" or "last mile" in that path.

including any health care providers or emergency services organizations that lost service.

To begin work necessary to resume financial market operations, telecommunications carriers then had to obtain generators and use emergency power to support network operations and to coordinate with financial institutions to facilitate the resumption of stock exchange activities by September 17, 2001. For example, Verizon managers met with representatives of the New York Stock Exchange (NYSE), major brokerage houses, the Securities and Exchange Commission (SEC), and the New York Federal Reserve to plot that restoration effort. They also had to start the extensive switching, cabling, and network electronics restoration activities, conduct broader customer outreach, and, where possible, provide alternative telecommunications services in the affected area.

Telecommunications Companies Overcame Numerous Restoration Challenges

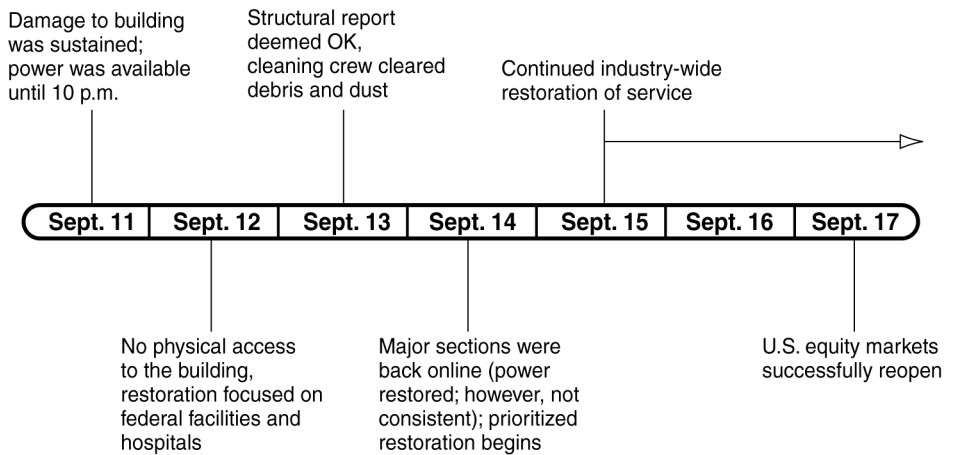
Telecommunications carriers faced two overall challenges in restoring connectivity to financial market customers. First, access to lower Manhattan was restricted, with evacuation zones established on September 11 and in place for several weeks because of immediate rescue and recovery efforts at the attack site as well as continuing safety and security concerns within the area. Therefore, telecommunications carriers had to coordinate work crew access to the area for restoration activities. WorldCom managers reported to us that the greatest difficulty they encountered during the first few days of the crisis was being unable to determine who was in charge of area access control points and who could approve movement of needed materials. Obtaining complete clearance through the various local, state, and federal officials, including the National Guard, took WorldCom about 2 days. According to Verizon managers, gaining access to the area required their most senior executives to request resolution from the Mayor's Office.

Safety and environmental issues also impeded initial restoration efforts. Specifically, according to Verizon managers, their efforts to assess damage and begin repairs on the 140 West Street facilities were initially delayed by concerns over the structural integrity of the facility and other buildings nearby. Furthermore, in the immediate aftermath of the attacks, firefighters used the Verizon facility to extinguish fires still burning in the area and contributed to the flooding of the facility's cable vaults. The loss of electrical power in that area also hampered initial restoration efforts. In addition, Verizon's efforts were delayed because they had to install a new air-pressure system after the existing system was damaged. Verizon needed

**Appendix I
Telecommunications Providers and Others
Cooperated to Overcome Damage to
Telecommunications Infrastructure**

this system to protect underground circuits in that area from water that could enter cabling. The time line in figure 13 illustrates major challenges during restoration efforts at 140 West Street.

Figure 13: Verizon Overcame Major Challenges During 140 West Street Restoration Efforts



Source: Verizon Communications, Inc.

Restoring services from the 140 West Street facility required considerable effort under difficult conditions. Verizon technicians were unable to access telecommunications manholes at 140 West Street until 30-foot-high piles of debris were removed. Because of the debris and extensive damage within the building, Verizon staff temporarily ran cables over the ground and around damaged cabling to quickly restore services. Because of damage to the cable vault, a new cable vault was reconstructed on the first floor, and cables were run up the side of the building to the fifth and eighth floors. (See fig. 9 in ch. 2.)

AT&T's restoration effort focused on replacing telecommunications services that were routed through its central office in the World Trade Center complex, which collapsed on September 11. AT&T supported and cooperated with Federal Emergency Management Agency and local authorities to establish emergency communications to the affected areas and with financial institutions to facilitate resumption of NYSE operations. AT&T established a temporary mobile central office by deploying tractor-trailers with necessary equipment to northern New Jersey. AT&T used

**Appendix I
Telecommunications Providers and Others
Cooperated to Overcome Damage to
Telecommunications Infrastructure**

telecommunications lines in the tunnels to New Jersey to link service in Manhattan to that temporary facility.

**City Officials Helped
Coordinate Carrier
Restoration Efforts**

New York City agencies played a key role in the restoration process, collaborating with carriers, assisting in prioritizing service recovery requirements, and coordinating restoration efforts among carriers. To coordinate these efforts, the New York City Department of Information Technology and Telecommunications (DOITT) invoked the City's Mutual Aid and Restoration Consortium (MARC) agreement. MARC required telecommunications franchisees in New York City to assist in the delivery of alternative voice and data services to essential city government offices and operations in an emergency. DOITT coordinated a series of bridge conference calls that included approximately 20 telecommunications service providers and facilitated communication and coordination of restoration efforts. These twice-daily calls allowed city officials to help set telecommunications restoration priorities and also gave carriers an opportunity to share information and offer assistance. Although not a party to the MARC agreement, wireless communications carriers and staff from the federal National Communications System (NCS), which is responsible for administering federal national security and emergency preparedness telecommunications programs, also participated in these calls.⁶

⁶NCS, which includes representatives from 22 federal departments and agencies, is responsible for ensuring the availability of telecommunications infrastructure for entities with national security and emergency preparedness responsibilities. Formed in 1962 following the communications difficulties during the Cuban Missile Crisis, NCS provides emergency communications for the federal government during all emergencies and international crises.

Regulator and Market Participants Are Working to Improve Crisis Response and Telecommunications Resiliency

Financial regulators and market participants have begun efforts to ensure that they are better able to respond to future crises. The financial sector is one of the key sectors being addressed by organizations responsible for ensuring that the nation's critical infrastructure is protected. In response to some of the problems that occurred after September 11, government and industry are working together to develop plans or put systems into place for accessing affected areas and to improve communication and information flow during crises. In response to difficulties that market participants experienced in the aftermath of the attacks, regulators and market participants are working to ensure that financial market organizations receive appropriate priority for telecommunications restoration and transmission. Market participants and telecommunications providers are also working to facilitate access by critical personnel to affected sites and to improve the resiliency of the telecommunications networks serving financial markets.

New Organizations Will Increase the Extent to Which Critical Infrastructure Protection Efforts Address the Financial Sector

New organizations have been formed to further address critical infrastructure in the financial sector. In 1998, a Presidential Decision Directive described a strategy for cooperative efforts by government and the private sector to protect critical, computer-dependent operations in key sectors of the U.S. economy, including banking and finance. The directive designated the Department of the Treasury (Treasury) as the lead agency for the banking and financial sector. Treasury was to work with the private-sector and government organizations to develop a plan to assess infrastructure vulnerabilities and develop mitigation strategies for each of the identified vulnerabilities.¹ Treasury has taken various actions, including establishing a committee to develop national strategy for the sector and creating a Financial Services Information Sharing and Analysis Center in 1999 to share information about threats and incidents and provide access to subject matter expertise and other relevant information.

Recently, additional organizations have been created to address threats to the critical assets of the U.S. financial sector. In October 2001, the President's Critical Infrastructure Protection Board has formed the Financial and Banking Information Infrastructure Committee (FBIIC), which includes the financial regulators responsible for securities, futures,

¹The other sectors included the nation's water supply, transportation, emergency and law enforcement services, public health services, electric power, and oil and gas production and storage.

banking, insurance, and government-sponsored enterprises, to assist the Board in ensuring that critical infrastructure in the financial markets is addressed. FBIIC acts as the lead coordinating organization between the financial services industry and the federal entities leading the effort to protect the critical infrastructure and key assets of the financial services industry. Another new organization consisting of private-sector organizations, the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, has also been created to coordinate sectorwide activities to improve critical infrastructure protection and homeland security. Its members include representatives from the Securities Industry, Bond Market, and American Bankers Associations, and individual market participants, including the stock exchanges, clearing organizations, broker-dealers, and banks. The status of efforts that address critical infrastructure protection in the financial sector are discussed more fully in our January 2003 report.²

Regulators and Market Participants Are Acting to Improve Crisis Response

In response to some of the problems that occurred in the aftermath of September 11, government and industry are working together to develop plans or put systems into place for accessing affected areas and improve communication and information flow during crises. As we described in chapter 2, the terrorist attacks on September 11, 2001, resulted in access restrictions over a large area of lower Manhattan. Initially only emergency personnel, law enforcement officials, and other first responders could enter the area. Staff at some market participants experienced difficulties in obtaining access to their facilities. For example, staff at one electronic communication network (ECN) said they could not access their offices because the authorities responsible for controlling access to the area had not heard of their organization. Representatives of some of the firms with whom we met that had offices in the affected area told us that obtaining access was sometimes difficult because different entities, such as the local police or the National Guard, were responsible for controlling access points during the week. Moreover, these entities did not necessarily have identical lists showing which personnel were authorized to enter the area. In addition, the process for gaining authorized access to the area was unclear. In some cases, financial market organization staff told us they relied on personal contacts with governmental officials or the New York Police Department to gain access to their facilities.

²U.S. General Accounting Office, *Critical Infrastructure Protection: Efforts of Financial Services Sector to Address Cyber Threats*, [GAO-03-173](#) (Washington, D.C.: Jan. 30, 2003).

**Appendix II
Regulator and Market Participants Are
Working to Improve Crisis Response and
Telecommunications Resiliency**

To avoid or mitigate future access difficulties, New York City's Office of Emergency Management, the Mayor's Office, and private-sector organizations were developing a more structured process to control access to the city during crises. These organizations are working on a project started by the Business Network of Emergency Resources (BNET). BNET is a nonprofit organization based in Buffalo, New York, that has developed emergency management plans for businesses throughout New York State to address snowstorms and other emergencies. The members of BNET developed the Corporate Emergency Access System, which will assist local businesses in entering restricted areas during emergencies. Under this system, organizations are to designate essential employees that should have access to their companies' facilities during emergencies if necessary. BNET will issue photo identification cards to employees deemed essential by participating organizations. This initiative is awaiting approval from the New York City Mayor's Office.

As a result of some inconsistencies in information dissemination to market participants in the aftermath of the attacks, financial regulators and some market participants have several efforts under way to improve communications during crises. Following the September terrorist attacks, some financial market participants were unsure of who was in charge and how the decision-making process would work to reopen the markets in an appropriate manner. For example one firm reported that it was not initially made aware of or was unable to participate in specific conference calls that were coordinated by federal regulators, calls in which decisions were made on when the markets would reopen. A few firms also reported learning of decisions via reports televised on CNN.

Since the attacks, market participants have created new mechanisms for communicating during crises. Securities and Exchange Commission (SEC) staff noted that having all interested organizations participating in all key conference calls in which decisions are being made is not possible. SEC staff told us that they believed that as many of the important market participants that could be accommodated did participate in the key calls and major meetings. SEC staff noted that new ways to ensure adequate information dissemination have been created. For example, in future events, the Security Industry Association's (SIA) newly established command center could facilitate communications between regulators and market participants. This command center can serve as a central point for communicating the status of participants and the markets, assist in coordinating industry response activities, and provide for liaison to and among city, state, and federal bodies before, during, and after a disaster.

SIA officials told us this command center has already been successfully used to coordinate information during a recent power outage in New York City's financial district.

Numerous Initiatives Are Under Way to Strengthen the Resiliency of Local Telecommunications Services

Financial regulators, market participants, and telecommunications providers also have efforts under way to improve access to and the resiliency of telecommunications services used by the markets. Financial regulators are expanding outreach to financial market participants to enroll them in programs designed to provide priority telecommunications restoration and service during crises. Telecommunications carriers also are increasing customer awareness of services that can improve telecommunications reliability and recoverability and improving the physical security of their systems and continuity plans. Additionally, financial market participants are assessing weaknesses in their telecommunications infrastructure and designing and testing new network configurations. Finally, other national and local government plans, such as mutual aid agreements—designed to improve telecommunications recoverability—are under way.

Existing Programs Already Can Be Used to Increase Priority and Access to Telecommunications Services

An existing federal program allows financial market participants to receive telecommunications priority in crises. Under the Government Emergency Telecommunications Service (GETS) Program, participating staff receive a card that provides them with a code that can be dialed to increase the priority of telephone calls they place during crises. To better ensure that critical communication among financial market participants occurs, FBIIC issued an interim policy on the GETS Card Program in July 2002 that outlines how staff from financial institutions can obtain such cards. To qualify for GETS sponsorship, the FBIIC policy states that organizations must perform functions critical to the operation of key financial markets.

Another FBIIC telecommunications effort involves the Federal Communications Commission's (FCC) Telecommunications Service Priority (TSP) Program, which is used to identify and prioritize telecommunication services that support national security or emergency preparedness missions. Under TSP, private-sector organizations, through the sponsorship of a selected group of federal agencies, including SEC and the Federal Reserve, can have some of their key telecommunications circuits added to an inventory maintained by the National Communications

**Appendix II
Regulator and Market Participants Are
Working to Improve Crisis Response and
Telecommunications Resiliency**

Service (NCS).³ These circuits are then eligible for priority restoration in a disaster. In the aftermath of the attacks, about 10 financial institutions obtained prioritized restoration of 81 circuits and provisioning of 81 new circuits under the TSP program. Although only a small number of financial firms currently participate in TSP, these firms are responsible for a substantial percentage of the daily funds transfer activity in the United States. For example, Federal Reserve staff said that financial institutions that account for about 90 percent of the total dollar volume of Fedwire and CHIPS payments, which are used to transfer large dollar-value payments among banks, have TSP-sponsored circuits. However, FBIIC members have concluded that other important financial market participants should be included in TSP. As a result, they have initiated outreach efforts to increase awareness of TSP and other government programs designed to provide priority service in emergencies and are currently developing a policy that will outline the requirements for financial firms to participate in TSP.

September 11 also illustrated that regulators would have to be flexible in setting telecommunications restoration priorities because the firms that are critical to the markets after a disaster may not have been previously identified or categorized as important. For example, staff at one of the few inter-dealer brokers (IDB) in the government securities markets that was capable of conducting operations after the attacks, said they had not been aware of the TSP program and had trouble getting priority provisioning for additional telecommunications capabilities following the attacks. However, after the attacks, this firm's operations became critical to the government securities market because so few other firms were capable of resuming operations quickly. This IDB eventually got assistance from the White House and SEC in obtaining the appropriate priority. Yet, prior to this event, this firm may not have been considered a strong candidate for TSP because it had relatively low trading volumes. To address this type of situation in the future, regulators said that a former Federal Reserve staff member has been placed on site at NCS, which fields requests for TSP restoration. This person will act as a liaison with the financial regulators and NCS.

³NCS consists of 22 federal member departments and agencies and is responsible for ensuring the availability of telecommunications infrastructure for entities with national security and emergency preparedness responsibilities. Formed in 1962 following the communications difficulties during the Cuban Missile Crisis, NCS provides emergency communications for the federal government during all emergencies and international crises.

Additional efforts by regulators and market participants are under way. Federal Reserve staff told us that they met in November 2002 with representatives of the National Security Telecommunications Advisory Committee to discuss the reliance of the financial and other critical sectors on telecommunications infrastructure. At this meeting, they discussed concerns over concentration and security issues relating to telecommunications facilities. In December 2002, this group established a working group to identify and assess telecommunication infrastructure issues and Federal Reserve staff told us that the financial sector would work with this group to develop recommendations.

**Carriers Offer Services to
Improve Customer
Continuity and Are
Improving Their Continuity
Plans and Strengthening
Local Service Infrastructure**

Telecommunications carriers are taking steps to improve their customers' awareness of services that can improve the reliability and recoverability of existing telecommunications, including the use of fiber-optic networks and other approaches that provide more reliable access to public networks, and services that help to recover failed connections. While each of these services will protect against some outages, they may not have prevented the extensive disruptions that occurred on September 11, 2001. Carriers also offer services that customers can use to redirect their switched telecommunications services, such as voice calls, to another business location, either in response to a crisis or for more general business reasons, such as receiving after-hours calls. On the basis of customer information stored in the carrier's central office switching system, these services can be used individually or in conjunction with other continuity services to rapidly route communications around failure points in a customer's communications path. However, because this service primarily protects switched communications services, it would not protect or more rapidly restore services delivered using dedicated, nonswitched communications lines.

Telecommunications carriers are also working to improve their basic services in two ways: by improving their continuity planning efforts and by strengthening the reliability of their networks. For example, AT&T had previously made substantial investments in its contingency capability, tested that capability on a quarterly basis, and was able to exercise that capability to process communications traffic within 72 hours of the World Trade Center attacks. Although Verizon reported that it also had plans in place prior to the attacks that aided its recovery efforts, Verizon is actively working to strengthen its internal continuity practices. Verizon is revising its January 1996 Central Office Disaster Recovery Plan based on lessons learned, and, at the same time, developing business unit continuity plans to

identify critical processes and operation support systems and harden control centers supporting emergency management activities. Verizon contingency managers indicated that this latter effort, which was about 75 percent complete in July 2002, would be the basis for developing mission-critical control plans to address relocation contingencies and building plans to address facility-specific evacuation, fire, and rescue situations. These efforts will then feed into Verizon's regional preparedness plans.

Verizon and AT&T are also taking steps to improve the reliability and resiliency of their networks as they rebuild damaged infrastructure. For example, Verizon plans to serve the financial district with more central offices to improve network redundancy and diversity. Verizon also plans to build more fiber-optic rings in its local network and use more modern synchronous optical network (SONET) technology in those networks.⁴ Verizon estimates its total reconstruction costs to be more than \$1.4 billion. In support of its long-term restoration effort, AT&T has also upgraded its fiber-optic networks and rebuilt two diverse central office facilities.

**Financial Market
Participants Are Also Taking
Steps to Promote More
Reliable
Telecommunications**

Financial market participants are also taking actions to reduce their vulnerability to future telecommunications disruptions. For example, a working group formed by senior telecommunications executives from major financial firms in lower Manhattan has completed an assessment of weaknesses revealed by the September 11 attacks and outlined ideas for making the local telecommunications infrastructure more reliable and resilient to outages.⁵

SIA has also taken the lead in designing and scheduling industrywide testing, so that major financial institutions, exchanges, and industry utilities can simultaneously activate work area recovery and data center recovery plans from alternate sites and gain confidence that their facilities work as envisioned in their plans. SIA currently plans for two phases of testing that focus on backup connectivity between industry participants. Phase 1 testing assumes an outage at the participant's primary facility. Phase 2 testing assumes that an event has occurred in a specific geographic

⁴Fiber optic cables consist of glass or plastic threads (fibers) that transmit information using light waves.

⁵*Building a 21st Century Telecom Infrastructure*, Lower Manhattan Telecommunications Users' Working Group Findings and Recommendations, August 2002.

**Appendix II
Regulator and Market Participants Are
Working to Improve Crisis Response and
Telecommunications Resiliency**

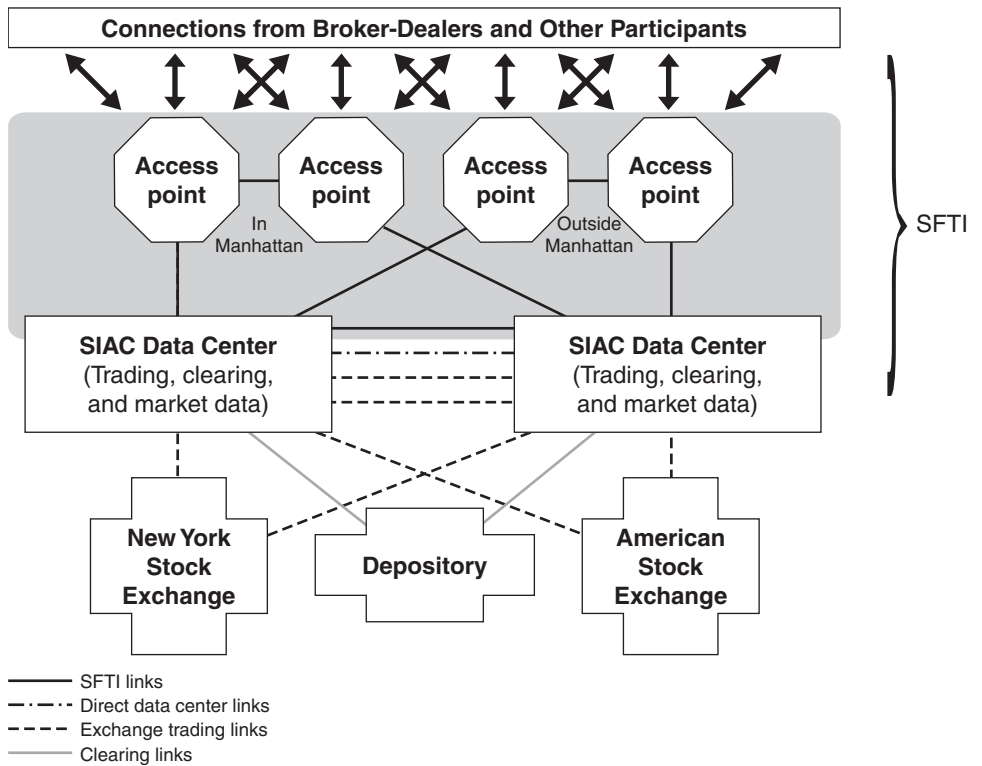
region causing disruption to supporting infrastructure (e.g., telecommunications and electrical power). In phase 1 tests, participants are required to test communications facilities between their own backup sites and the primary sites of critical parties. During phase 2 testing, all test participants with primary data centers and work area sites in designated geographic regions need to test recovery from backup or alternate sites.⁶

In addition to these actions, the financial industry has started work on a more resilient private networking platform that will transmit trading and clearing information among various market participants. The Securities Industry Automation Corporation (SIAC), which is a jointly owned subsidiary of the New York Stock Exchange and American Stock Exchange, is developing the network platform, known as the Secure Financial Transaction Infrastructure (SFTI). SFTI is intended to provide a more reliable and survivable private communications mechanism linking the exchanges, the clearing organization for securities, and broker-dealers. Whereas broker-dealers currently connect to SIAC through hundreds of individual connections, in the future they will connect to SFTI via four access points, which will be located at switching facilities served by multiple telecommunications providers. Figure 14 illustrates the connections among SFTI participants.

⁶Securities Industry Association Business Continuity Planning Committee Industry Testing Workgroup, "Plan for Industry Testing: Version 1," September 10, 2002.

**Appendix II
Regulator and Market Participants Are
Working to Improve Crisis Response and
Telecommunications Resiliency**

Figure 14: The SFTI Network Provides Redundant Connections



Source: Securities Industry Automation Corporation.

The traffic on SFTI will be transmitted over two high-bandwidth, fiber-optic rings. To provide physical diversity and promote survivability, two SFTI network access points would be located in Manhattan and two outside the New York metropolitan area. In this way, users with more than one operating location can connect these locations to SFTI at two distinct points on either of the two SFTI network rings, thus reducing the likelihood that a disaster would leave such participants unable to transmit trading or clearing information. SFTI will initially use network facilities provided by Con Edison Communications because that firm uses different rights-of-way

than other carriers in Manhattan.⁷ SIAC entered into service agreements with Con Edison Communications in September 2002, and planned to begin preliminary network testing in November 2002. After testing is complete, SIAC plans to initiate broader implementation, hoping to have all interested firms on the network within 2 years. SIAC plans to establish additional SFTI access nodes in Boston, Massachusetts, and Chicago, Illinois, to accommodate users in those cities.

**Other National and Local
Government Efforts
Intended to Increase
Telecommunications
Response and Resiliency**

The National Reliability and Interoperability Council (NRIC), a federal advisory council to the FCC, is examining ways to strengthen the resilience and recoverability of the nation's public telecommunications networks in light of the September 11 attacks. One NRIC subgroup will report on the viability of past or present mutual aid agreements and any additional perspectives that facilitate effective telecommunications recovery efforts. This subgroup also is preparing a template for mutual aid agreements for carriers, and examining if telecommunications technicians should be recognized as first responders to overcome the sort of access obstacles that hampered initial telecommunications recovery efforts in New York City. Additionally, the NRIC subgroup is examining how to operationally transfer communications traffic from the damaged facilities of one carrier to the facilities of another carrier with operating network capacity. Although such offers were made in September, Verizon was not able to leverage them because carriers did not have systems and processes in place that could facilitate inter-carrier transfers. In addition to these recovery issues, a second NRIC subgroup is assessing physical vulnerabilities and identifying existing and new best practices to both mitigate the effects of physical infrastructure attacks and restore services after such attacks. The NRIC subgroups are scheduled to complete work by March 2003.

New York City is leading an effort to enhance cooperation among telecommunications providers. In 1992, New York City established the Mutual Aid and Restoration Consortium (MARC) agreement, which is intended to ensure the continuity of services in the city under all

⁷Con Edison Communications, a wholly owned subsidiary of Consolidated Edison, Inc., builds and operates its own fiber-optic network providing data communications services and custom network solutions to multiple classes of customers, including telecommunications carriers, corporations, and Internet, cable, wireless, and video companies.

**Appendix II
Regulator and Market Participants Are
Working to Improve Crisis Response and
Telecommunications Resiliency**

reasonably foreseeable circumstances. Although this agreement expired at the end of 1998, the New York City Department of Information Technology and Telecommunications (DOITT) invoked it in the aftermath of the September 11 attacks to ensure that essential city government offices and operations would have adequate telecommunications service. DOITT coordinated a series of conference calls that included approximately 20 telecommunications service providers; these twice-daily calls allowed city officials to help set telecommunications restoration priorities and also gave carriers an opportunity to share information and offer assistance.

To ensure this agreement continues to function well, New York City officials are revising and expanding it. The new MARC agreement will formalize the roles of the Mayor's Office and the Office of Emergency Management and also will explicitly include wireless service providers who had not been mentioned in the 1992 agreement. Finally, the new draft also proposes using the Internet to make information more readily available to all parties.

Comments from Federal Reserve System



BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

STEPHEN R. MALPHRUS
STAFF DIRECTOR FOR MANAGEMENT

January 27, 2003

Ms. Davi M. D'Agostino, Director
Financial Markets and Community Investment
U.S. General Accounting Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. D'Agostino:

Thank you for the opportunity to comment on GAO's draft report *Potential Terrorists Attacks: Additional Actions Would Better Prepare Critical Financial Market Participants*. Addressing the risks posed by the events of September 11 is a priority for the Federal Reserve. As the draft report notes, we are working to improve the resilience of the financial system in several ways, including

1. In cooperation with banking and securities regulators, developing sound practices that focus on minimizing the immediate systemic effects of a wide-scale disruption on critical financial markets, and
2. Together with the other banking regulators, expanding guidance for banks on information security and business continuity.

Technical comments on the draft report were provided to GAO during a recent meeting. We appreciate the efforts of your staff to respond to our comments.

Sincerely,

A handwritten signature in cursive script, appearing to read "Steve Malphrus".

Mail Stop 50, Washington, DC 20551
Telephone: (202) 452-2801 • Internet: steve.malphrus@frb.gov • Facsimile: (202) 728-5832

Comments from the Securities and Exchange Commission



DIVISION OF
MARKET REGULATION

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

January 21, 2003

Ms. Davi M. D'Agostino
Director, Financial Markets
and Community Investment
United States General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. D'Agostino:

This letter responds to your request to review and comment on the draft report entitled Potential Terrorist Attacks: Additional Actions Would Better Prepare Critical Financial Market Participants, GAO-03-251. We appreciated the opportunity to meet with you and your colleagues to convey comments on the report and appreciate your willingness to address our comments in your report.

We share the GAO's views regarding the importance of emergency preparedness of the financial markets. As the report recognizes, we have been working actively with the trading markets and the major market participants to strengthen their resiliency. Accordingly, we generally agree with the report's principle that the financial markets should be prepared to resume trading in a timely, fair and orderly fashion following a catastrophe.

As we indicated in our meeting with you and your colleagues, we have some concerns with the recommendation that we ensure that broker-dealers implement sound business continuity practices to resume trading. Specifically, it should be recognized that a broker-dealer's provision of liquidity to the market is voluntary. Because risking capital and providing brokerage services are in essence business decisions, a broker-dealer's choice whether to continue to trade on an ongoing basis or in a crisis is not primarily a matter of government regulation; rather, it is governed by the costs involved, relationships with customers, and profitability. In contrast, when a significant trading market or broker-dealer has executed trades, it must process these outstanding trades promptly, in order to reduce financial exposures in the clearance system and reduce systemic risk. Similarly, broker-dealers should provide customers with access to funds and securities in their accounts as soon as is physically possible. We believe that business continuity planning expectations must reflect these various considerations.

With respect to the Commission's Automation Review Policy ("ARP") program, we agree with the GAO's recognition of the importance of market participants appropriately responding to ARP recommendations. As the Commission stated in ARP

Ms. Davi M. D'Agostino
January 21, 2003
Page 2

II,¹ we continue to assess whether rulemaking is appropriate in this area. In addition, subject to the availability of funding, we will consider recommending to the Chairman an expansion in the level of staffing and resources committed to the ARP program.

Regarding the discussion on pages 81 and 82 of the draft report, the GAO observes that ARP does not address how organizations should protect their entire organization from physical attacks. We note that the ARP policy statements did not envision organization-wide physical security to be a direct component of the ARP program; instead the focus was on securing IT resources. We are reviewing the references noted in the draft report regarding physical security and, based on mission, staffing, and workload, may consider broadening inspections to include organization-wide concerns. This effort will entail a significant resource commitment and hiring consultant expertise in this highly specialized area.

* * *

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

¹ Securities Exchange Act Release No. 29185 (May 9, 1991) [56 Fed. Reg. 22490].

GAO Contacts and Staff Acknowledgments

GAO Contacts

Davi M. D'Agostino (202) 512-8678
Cody J. Goebel (202) 512-8678

Acknowledgments

In addition to the individuals named above, Edward Alexander, Ron Beers, Lon Chin, Kevin Conway, Kirk Daubenspeck, Patrick Dugan, Edward Glagola, Daniel Hoy, Harold Lewis, Marc Molino, Thomas Payne, Robert Pollard, Jean-Paul Reveyoso, Barbara Roesmann, Derald Seid, Keith Slade, Eugene Stevens, Sindy Udell, and Daniel Wexler made key contributions to this report.

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**

