

September 2004

FINANCIAL MARKET PREPAREDNESS

Improvements Made,
but More Action
Needed to Prepare for
Wide-Scale Disasters



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-04-984](#), a report to the Committee on Energy and Commerce, House of Representatives

Why GAO Did This Study

In February 2003 reports, GAO identified actions needed to better prepare critical financial market participants for wide-scale disasters, such as terrorist attacks. To determine progress made since then, GAO assessed (1) actions that critical securities market organizations took to improve their ability to prevent and recover from disruptions, (2) actions that financial market and telecommunications industry participants took to improve telecommunications resiliency, (3) financial regulators' efforts to ensure the resiliency of the financial markets; and (4) SEC's efforts to improve its program for overseeing operations risks at certain market participants.

What GAO Recommends

GAO recommends that the Chairman, SEC, fully analyze the readiness of the securities markets to recover from major disruptions and work with industry to determine actions that would better prepare the markets to resume trading. This report also recommends actions to improve SEC's information technology oversight program, including establishing a time frame for proposing a rule making the program mandatory, increasing its resources, and continuing to assess the alignment of the program within SEC.

SEC generally agreed with the findings and recommendations of this report.

www.gao.gov/cgi-bin/getrpt?GAO-04-984.

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

FINANCIAL MARKET PREPAREDNESS

Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters

What GAO Found

The critical securities market organizations and market participants GAO reviewed had taken actions, since GAO's previous reports, to further reduce the risk that their operations would be disrupted by terrorist attacks or other disasters. For example, they had added physical barriers, enhanced protection from hackers, or established geographically diverse backup facilities. Still, some entities had limitations that increased the risk that a wide-scale disaster could disrupt their operations and, in turn, the ability of securities markets to operate. For example, three organizations were at a greater risk of disruption than others because of the proximity of their primary and backup facilities. In addition, four of the eight large trading firms GAO reviewed had all of their critical trading staff in single locations, putting them at greater risk than others of a single event incapacitating their trading operations. Geographic concentration of these firms could leave the markets without adequate liquidity for fair and efficient trading in a potential disaster.

Since GAO last reported, actions were taken to improve the resiliency of the telecommunications service critical to the markets, including creating a private network for routing data between broker-dealers and various markets. Maintaining telecommunications redundancy and diversity over time will remain a challenge. Financial market regulators also took steps that should reduce the potential that future disasters would disrupt the financial markets, such as issuing business continuity guidelines for financial market participants designed to reopen trading markets the next business day after a disruption. However, despite the risk posed by the concentration of broker-dealers' trading staffs, and the lack of regulations requiring broker-dealers' to be prepared to operate following a wide-scale disruption, SEC had not fully analyzed the extent to which these organizations would be able to resume trading following such a disruption.

Furthermore, while SEC has made some improvements to the voluntary program it uses to oversee the information security and business continuity at certain critical organizations, it has not taken steps to address key long-standing limitations. Despite past difficulties obtaining cooperation with recommendations and a lack of resources to conduct more frequent inspections, SEC had not proposed a rule making this program mandatory or increased the level of the program's resources—as GAO has previously recommended. In addition, SEC appeared to lack sufficient staff with expertise to ensure that the organizations in the program adequately addressed the issues identified in internal or external reviews, or to identify other important opportunities for improvement. Although SEC staff continue to assess the impact of a recent reorganization involving the programs staff, whether the current placement of the program within SEC is adequate for ensuring that the program receives sufficient resources is not yet clear.

Contents

Letter		1
	Results in Brief	3
	Background	7
	Critical Organizations Reduced Risks from Physical or Electronic Attacks, but Some Organizations Still Had Limitations That Increased Potential for Disruptions	8
	Steps Are Under Way to Meet Challenge of Improving the Resiliency of Telecommunications	17
	Federal Financial Regulators Took Actions to Improve the Readiness of Securities Markets, but Further Actions Needed	24
	SEC Took Some Actions to Enhance Its ARP Program but Has Not Addressed Other Limitation to Its Effectiveness	31
	Conclusions	36
	Recommendations for Executive Action	38
	Agency Comments and Our Evaluation	38

Appendixes

Appendix I: Objectives, Scope, and Methodology	41
Appendix II: Role of the Department of Homeland Security	45
Appendix III: Comments from the Federal Reserve	47
Appendix IV: Comments from the Securities and Exchange Commission	48
Appendix V: GAO Contacts and Staff Acknowledgments	50
GAO Contacts	50
Acknowledgments	50

Related GAO Products	51
-----------------------------	----

Abbreviations

ARP	Automation Review Policy
BCP	Business Continuity Plan
CBR	chemical, biological, and radiological
DHS	Department of Homeland Security
ECN	Electronic Communications Network
FBIIC	Financial and Banking Information Infrastructure Committee
FCC	Federal Communications Commission
FFIEC	Federal Financial Institutions Examination Council
FISCAM	Federal Information System Controls Audit Manual
FS/ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council
HSPD-7	Homeland Security Presidential Directive 7
IAIP	Information Analysis and Infrastructure Protection
MARC	Mutual Aid Restoration Consortium
NASD	National Association of Securities Dealers, Inc.
NASDAQ	Nasdaq Stock Market, Inc.
NCS	National Communications System
NRIC	National Reliability and Interoperability Council
NSTAC	National Security Telecommunications Advisory Committee
NYSE	New York Stock Exchange
OCC	Office of the Comptroller of the Currency
OCIE	Office of Compliance, Inspections, and Examinations
SEC	Securities and Exchange Commission
SFTI	Secure Financial Transaction Infrastructure
SIA	Securities Industry Association
SIAC	Securities Industry Automation Corporation
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. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, D.C. 20548

September 27, 2004

The Honorable Joe Barton, Chairman
The Honorable John D. Dingell, Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

The Honorable Fred Upton, Chairman
The Honorable Edward J. Markey, Ranking Minority Member
Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
House of Representatives

The Honorable Cliff Stearns, Chairman
The Honorable Jan Schakowsky, Ranking Minority Member
Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
House of Representatives

The massive destruction to property and supporting utility infrastructure resulting from the September 11, 2001, terrorist attacks on the World Trade Center exposed the vulnerability of the financial markets to disruption by such events. In February 2003, we reported that critical financial market participants and regulators took many actions to reduce the risk that such disasters would disrupt the markets' operations in the future.¹ However, we also reported that some critical market participants still had limitations in their physical security protections or business continuity capabilities that increased their risk of being disrupted. In addition, we found that financial regulators had begun to take steps—such as issuing draft recovery goals and best practices for entities that perform the critical clearing and settlement functions that ensure that ownership and payments are transferred after trades occur—to reduce the likelihood that future disasters would lead to widespread payment defaults. Nevertheless, we also reported that regulators could take further actions to better ensure that trading could resume in a timely manner after such events. Thus, in our

¹See GAO, *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, [GAO-03-251](#) (Washington, D.C.: Feb. 12, 2003) and *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, [GAO-03-414](#) (Washington, D.C.: Feb. 12, 2003). Because these reports provide identical information, for simplicity, we will refer to them throughout this report as our 2003 report.

2003 report, we recommended that the Securities and Exchange Commission (SEC) work with industry to improve the preparedness of the financial sector to resume operations after future disruptions.

To further improve the preparedness of securities organizations, we also made recommendations to SEC to improve the Automation Review Policy (ARP) program that it uses to oversee security and operations continuity issues at exchanges, clearing organizations, and electronic communications networks (ECN), which are electronic venues for matching and executing orders to trade securities. Finally, we recommended that SEC make compliance with ARP mandatory and, if possible, increase the level of staffing and resources committed to the program.

Because of ongoing concerns about our nation's vulnerability to terrorist attacks, you asked that we review progress made since our previous report by (1) securities market organizations, including exchanges and clearing organizations; (2) market participants, such as key banks and broker-dealers; and (3) financial regulators to reduce the likelihood of potential terrorist attacks and other disasters disrupting market operations. You also asked us to report on the progress that SEC has made in responding to our recommendations of developing goals, strategies, and business continuity practices that could better ensure that market participants, which are needed for trading activities to resume, would be prepared for future disasters. In addition, you asked that we review the actions SEC has taken to improve the ARP program. Specifically, we assessed (1) actions that critical securities market organizations and key trading or clearing firms undertook to reduce their risk of disruption from terrorist attacks or other disasters; (2) steps that financial market participants, telecommunications industry organizations, and others took to improve the resiliency of telecommunications systems; (3) financial regulators' efforts to ensure the resiliency of the financial markets; and (4) the progress SEC has made in improving the ARP program.

In performing our follow-up work, we reviewed regulatory and industry documents and interviewed staff from broker-dealers, banks, regulators, telecommunications providers, industry associations, and other organizations. We visited seven organizations that we categorized as "critical," based on our consideration of whether viable immediate substitutes existed for the products or services they offered or whether the functions they performed were essential for the overall ability of the U.S. securities markets to continue operations. We inspected various physical

and electronic security measures at these seven organizations and reviewed their business continuity capabilities. In assessing the organizations' physical and electronic security and business continuity efforts, we used criteria that were either established by regulators or were generally accepted by government or industry. For our reviews, we relied on documentation and descriptions provided by market participants and regulators and reviews conducted by other organizations. When feasible, we also directly observed controls in place for physical security, electronic security, and business continuity at the organizations assessed. We did not test these controls by attempting to gain unauthorized entry or access to facilities or information systems, neither did we directly observe testing of business continuity capabilities. We also discussed the business continuity capabilities and improvements made by eight large broker dealers and banks that collectively represented a significant portion of trading and clearing volume on U.S. securities markets. In addition, we reviewed the efforts that financial market regulators, industry associations, and telecommunications carriers and organizations took to improve the resiliency of the financial markets. We performed our work from September 2003 through August 2004 in accordance with generally accepted government auditing standards. For security reasons, we did not include the names of the organizations we reviewed, their functions, or their locations in this report.

Results in Brief

Since our 2003 report, all of the critical securities market organizations and trading firms we reviewed further reduced the risk they faced from physical or electronic attacks and improved their ability to recover from such events. For example, the organizations had reduced risks by adding physical barriers around their facilities, enhancing protection from hackers, or establishing geographically diverse backup facilities. However, three of the seven organizations, which we determined to be critical to the functioning of the securities markets, faced increased risk of operations disruptions because of limitations in their business continuity capabilities. Because these three organizations had backup operating sites located within the same geographic area as their primary facilities, they were at greater risk than the other organizations that a single, wide-scale event

could prevent them from accessing or operating from either site.² One of these three organizations also faced an increased risk that its operations could be disrupted because it had not yet developed procedures to ensure that staff capable of conducting its critical operations would be available if an attack or other event incapacitated personnel at its primary site. Each of the seven critical organizations we reviewed also improved the security of their information systems and networks. In addition, we reviewed eight broker-dealers and banks that conduct significant portions of U.S. securities markets trading and clearing activities, and we found that these firms also had further reduced the risk that potential future disasters would disrupt their operations. However, four of these key firms continued to face greater risk than others because they had concentrated key trading staff in single locations. Officials at some of these firms said they recognized this increased risk, but they said the decreased efficiency and increased costs that would be associated with splitting or rotating these staff exceeded the risk of disruption. Nevertheless, a wide-scale disaster could incapacitate trading staff at a sufficient number of firms to prevent the timely resumption of fair and orderly trading in the securities markets because a number of these firms were in the same geographic area.

Securities market participants, telecommunication carriers and industry organizations, and government agencies also worked to improve the resiliency of telecommunications services critical to the financial sector. Many firms learned in the aftermath of the September 2001 attacks that their telecommunications services were not as resilient as expected because, in some cases, their communications carriers had rerouted their lines over time to follow similar physical paths. In response to the challenge of maintaining diversity, a new private communications network has been created to provide more reliable and resilient communications for the broker-dealers, exchanges, and clearing organizations that participate in securities and other markets. In addition, federal financial regulators and telecommunications organizations have been working together on initiatives to enhance telecommunications resiliency for the financial sector, such as identifying best practices and sponsoring financial market participants in federal programs that increase the priority for restoration of

²Federal financial regulators have defined a wide-scale disruption as 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; or that results in a wide-scale evacuation or inaccessibility of the population within normal commuting range of the disruption's origin.

damaged communications circuits. Further, large telecommunications carriers serving the financial district in Manhattan also have been taking steps to improve the diversity of their network infrastructures and are offering services that may improve their customers' communications resiliency.

Since our 2003 report, financial market regulators have worked to reduce the degree to which potential future disasters would disrupt the financial markets. The regulators for banks and securities firms issued joint guidance that directs key clearing and settlement organizations to implement business continuity best practices—including having geographically diverse backup capabilities—by the end of 2004 that will enable them to resume clearance and settlement activities within 4 hours following a wide-scale disruption. To better ensure that trading activities would also resume without undue delay, SEC also issued a policy statement that expects exchanges and ECNs to implement certain business continuity practices by the end of 2004. Specifically, these organizations would have to have the capability to resume trading the next business day after a wide-scale disaster. In addition, the New York Stock Exchange (NYSE) and the National Association of Securities Dealers (NASD) adopted new rules that require their member broker-dealers to have business continuity plans in place by September 2004. As we reported in 2003, part of the delay in reopening the trading markets after the September 2001 attacks was attributable to the difficulties that broker-dealers faced in recovering their trading operations. SEC officials told us that because trading is a voluntary activity, and SEC cannot compel broker-dealers to participate in the markets to any degree, none of the new regulatory guidance requires trading firms to develop capabilities to resume operations following such events. Although several of the firms that account for a significant amount of securities trading volume face increased risk that a wide-scale disaster could disrupt their trading operations, SEC had not yet completely analyzed whether a sufficient number of trading firms are likely to be ready to resume trading after a wide-scale disruption. In addition, SEC had not completely analyzed whether firms located outside the affected area would be able and willing to conduct trading at a level necessary to ensure sufficiently fair and liquid markets if the currently most active firms were not.

While SEC had taken some steps to improve its ARP program, the agency had yet to address limitations that have hampered the effectiveness of the program. SEC staff now more frequently contact the entities they review—exchanges, clearing organizations, and ECNs—to determine

whether appropriate actions are being taken in response to recommendations made by ARP staff. Although in the past, SEC has had problems with organizations cooperating with some ARP recommendations and other program components, SEC staff said that currently cooperation has improved. However, they also agreed that a rule making compliance with ARP guidelines mandatory—as we had recommended in our 2003 report—would help ensure future compliance with the ARP program. While such a rule had been drafted, it had not yet been presented to the Commission. In addition, despite recommendations in our prior reports to increase ARP staff to do more frequent and in-depth examinations and the increased resources made available to the agency, SEC had not yet significantly increased the resources devoted to the ARP program. Further, while internal and external reviews of the operations of exchanges, clearing organizations, and ECNs are key to the effectiveness of the ARP program, we found instances where SEC had not ensured that the entities took adequate and timely steps to address the concerns identified in those reviews. Moreover, our work raised additional concerns that the ARP programs’ staff expertise and approach may not adequately address information security issues at the organizations it reviews. For example, at the critical organizations that we reviewed, we identified important additional opportunities for improvements in information security that internal or external reviewers or ARP staff had not identified. The ARP program was moved to a new office within the Division of Market Regulation in November 2003, and SEC staff told us this move has been beneficial but that they continue to assess its impact. However, whether the current placement of the program within SEC is adequate for ensuring that the ARP program receives sufficient resources and attention is not yet clear.

This report includes recommendations to the SEC Chairman to fully analyze the readiness of the securities markets to resume trading after potential future disasters, ensure that the ARP program has sufficient staff with appropriate expertise to review information security issues, and continue to assess the alignment of the ARP program within SEC’s organizational structure. In commenting on a draft of this report, SEC generally concurred with our recommendations and described the actions it planned to take to implement them.

Background

Customer orders for stocks and options, including those from individual investors and from institutions such as mutual funds, are generally routed through a broker-dealer and executed at one of the many exchanges located in the United States. 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 and is performed by separate clearing organizations for stocks and for options. A depository maintains records of institutional ownership for the bulk of the securities traded in the United States. Banks also participate in the U.S. securities markets by acting as clearing banks that maintain accounts for broker-dealers to accept and make payments for these firms' securities activities. Payments for corporate and government securities transactions, as well as for business and consumer transactions, are transferred by payment system processors, including those operated by the Board of Governors of the Federal Reserve (Federal Reserve) and private organizations. Virtually all of the information processed is transferred between parties via telecommunications systems; and as a result, the securities markets depend heavily on its supporting telecommunications infrastructure.

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. Some are more important than others because they offer unique products or perform vital services. For example, markets cannot function without the activities performed by clearing organizations; and in some cases, only one clearing organization exists for particular products. In addition, other market participants are critical to the overall market functioning because they consolidate and distribute price quotations or information on executed trades. Other participants may be critical to the overall functioning of the markets only in the aggregate. For example, if one of the thousands of broker-dealers in the United States 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. However, a small number of large broker-dealers account for sizeable portions of the daily trading volume on many exchanges. If several of these large firms were unable or unwilling to operate, the markets might not have sufficient trading volume to function in an orderly or fair way.

Several federal organizations oversee the various securities market participants.³ SEC regulates the stock and options exchanges and the clearing organizations for those products. In addition, SEC regulates the broker-dealers that trade on those markets and other participants, such as mutual funds, which are active investors. The exchanges also have responsibilities as self-regulatory organizations 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 the Department of the Treasury (Treasury) also plays a role. Treasury issues rules pertaining to securities market, but SEC or the bank regulators are responsible for conducting examinations to ensure that these rules are followed. Additionally, 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.

Critical Organizations Reduced Risks from Physical or Electronic Attacks, but Some Organizations Still Had Limitations That Increased Potential for Disruptions

Critical organizations and other trading and clearing firms improved their readiness for future terrorist attacks or other disasters in several ways, but some still remained at greater risk of disruption than others. For example, since our 2003 report, all of the seven critical organizations we reviewed reduced risks by adding physical barriers around their facilities, enhancing protection from hackers, or establishing geographically diverse backup facilities. However, several organizations still faced an increased risk of disruption from potential future attacks, either because of the location of their backup facilities or because they have not taken steps to better ensure the availability of critical staff. The key broker-dealers and banks that conduct significant trading and clearing activities that we reviewed had also improved their business continuity capabilities, but some were still at greater risk of disruption than others due to the concentration of key trading staff in single locations. Working together through industry

³While the Department of Homeland Security is responsible for coordinating all efforts to protect the nation against terrorist attacks, Homeland Security Presidential Directive 7 (HSPD-7) designates the Department of the Treasury as the sector-specific federal agency responsible for coordinating such efforts within the banking and finance sector. Treasury coordinates with and reports to the Department of Homeland Security on its efforts. See appendix II for further information.

associations, market participants also improved their ability to withstand future disasters by, for example, establishing crisis command centers.

Critical Organizations Further Improved Physical and Electronic Security

Since our previous report, almost all of the critical organizations took steps to improve their physical and electronic security. Physical security encompasses measures such as installing physical barriers around buildings, screening people and objects, and using employee and visitor identification systems. We assessed the organizations' physical security using standards and best practices developed by the Department of Justice.⁴ For example, as a deterrent to potential attacks, one organization increased the number of armed security officers that protect the perimeter of its facility. These security personnel are also now clad in military-style uniforms and possess greater firepower than they did previously. In addition, this organization installed additional video cameras to allow it to monitor more locations around its facility. Another organization we reviewed had installed new perimeter barriers and X-ray equipment outside of its facility to better protect its lobby and other interior spaces. Four of the critical organizations we reviewed still faced increased risks in their physical security, such as an inability to control vehicular traffic around their primary facility, which put them at greater risk of disruption from potential physical attacks than other organizations. However, each of these four organizations also had geographically diverse backup facilities capable of conducting some or all of the organization's critical operations, mitigating the effect of a disruption at the primary facility.

All seven organizations had also implemented countermeasures to mitigate chemical, biological, and radiological (CBR) threats. For example, each organization had identified its facilities' outdoor air intakes, which can be highly vulnerable to CBR attacks, and took steps to prevent access to them. Such steps included installing locks, video cameras, security lighting, and intrusion detection sensors in order to establish a security zone around the air intakes. The organizations also took actions to prevent public or unauthorized access to areas that provide access to centralized mechanical

⁴See 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 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. These measures are more geared to protect against an attack such as a vehicle or package bomb rather than an airborne attack.

systems, including heating, ventilation, and air conditioning equipment. Finally, some organizations also isolated their lobbies, mail processing areas, and loading docks.

An effective physical security program includes periodic testing of controls such as reviews of security guard performance outside of normal business hours, attempts to bring in prohibited items (such as weapons), and review of employees' use of access to restricted and sensitive areas. Periodic monitoring of such controls not only provides a valuable means of identifying areas of noncompliance or previously undetected vulnerabilities, but can also serve to remind employees of their security responsibilities and demonstrate management's commitment to security. Each of the organizations we visited performed these types of tests on a periodic basis.

The critical organizations also continued to invest in information security measures to reduce the risk that their operations would be disrupted by electronic attacks. Electronic attacks can come in different forms and include attacks in which persons (such as hackers) attempt to gain unauthorized access to a specific organization or system or attacks by computer programs or codes, such as viruses or worms. We applied criteria from the Federal Information System Controls Audit Manual, as well as other federal guidelines and industry best practices, to assess the organizations' information security. For more information on the scope of our assessment, please see appendix I. All of the organizations we reviewed enhanced protections against unauthorized outside access to their computer systems. For example, one organization increased the coverage of its intrusion detection and prevention systems to better monitor and address attacks by outsiders. Some of the organizations we reviewed also had invested in more secure technologies. For example, one organization put in place a new multitiered external network, which provides multiple layers of security. During our reviews, we also identified and discussed with these organizations additional actions they could take to further improve their information security.

Critical Organizations Improved Their Ability to Recover from Disruptions, but Some Faced Limitations That Increased Risks

All the critical organizations had also further increased their ability to recover from attacks or other disasters since our 2003 report, but some still had limitations in their business continuity capabilities that increased their risk of disruption. Since our report, these organizations also have more specific standards against which to measure their capabilities because federal financial regulators have issued business continuity guidelines and

principles that set expectations for these organizations.⁵ These regulatory guidelines direct the organizations to establish geographically diverse backup capabilities and state that the operation of a backup site should not be impaired by a wide-scale evacuation at the primary site or the inaccessibility of the staff. Although the guidance does not specify a minimum distance between primary and backup facilities, regulators state that such facilities should not rely on the same infrastructure components, such as transportation, telecommunications, water supply, and power supply.

As of May 2004, four of the seven critical organizations had geographically dispersed backup sites that their officials indicated were capable of conducting the organizations' critical operations. Each backup site was located at a considerable distance from the organizations' primary sites—ranging from almost 300 miles to over 1,100 miles. However, as of June 2004, the remaining three critical organizations that we noted in our previous report as lacking geographic separation between their primary and backup facilities did not have geographically diverse backup facilities capable of assuming all critical operations. Instead, these three organizations' current backup facilities were located within the same geographic area as their primary sites (although, as discussed below, one organization had a geographically diverse facility that it could use to run some of its critical applications). Officials at one organization said that these facilities do not depend on the same infrastructure components as their primary facilities; although, in some cases, they would depend on the same transportation system. Although having backup sites does reduce the risk that these organizations' operations would be disrupted in future attacks, both primary and backup facilities could be affected by wide-scale events, and thus, these organizations faced an increased level of risk of operational disruptions.

However, officials at the three critical organizations that lacked geographically dispersed backup sites were reducing the risks resulting from the proximity of their primary and backup facilities. One organization established a geographically diverse backup site, and as of June 2004, had the ability to run some of its critical operations from that site. Officials at this organization anticipated being able to conduct all of its critical operations from the new site by the end of 2005. To reduce the risk arising from certain types of events, the other two organizations had begun work

⁵We discuss these guidelines in more detail later in this report.

to establish management systems that would allow them to operate the hardware and systems at their primary sites from geographically remote locations. Federal financial regulators have stated that having a backup site that is fully capable of operating all critical functions is necessary for organizations to ensure that they can meet regulators' recovery objectives. (We discuss recovery objectives more fully later in this report.) However, these organizations' remote management capabilities, which both intended to have in place by the end of 2004, would allow them to continue operating under disaster scenarios in which their facilities were not damaged but were rendered physically inaccessible for public safety or other reasons. As of August 2004, one of these two organizations had a plan to implement a geographically diverse backup site by April 2005. The other organization was considering alternatives for being able to recover its operations in geographically dispersed locations but had not developed any definite plans.

Additionally, at the time we conducted this review, six of the seven organizations had arrangements in place that appear to ensure the availability of critical staff. Organizations also can enhance business continuity capabilities following a disaster by implementing plans to ensure the availability of key staff, if staff who perform critical activities at a primary facility become incapacitated. For example, one organization rotated its critical staff among multiple locations, ensuring that all such staff were never in the same location at the same time. However, one of the seven organizations had not developed a formal plan for ensuring the availability of key staff. Officials at this organization said they believed that a sufficient number staff necessary to conduct critical operations were not at the primary facility at any one time for a variety of reasons, including vacations and business travel. However, they had no formal plan to ensure that sufficient numbers of trained staff would be available should staff at the primary facility be lost. In July 2004, officials from this organization said they were seeking to have such a plan in place in the near future. This particular organization already has faced an increased risk of disruption because it was also one of the three organizations that did not yet have a geographically diverse backup facility. While this organization had improved its physical security, which can help protect an organization's primary facility as well as its critical staff, it was still at greater risk of disruption than other critical organizations.

Further, all seven organizations that we reviewed appeared to be following sound practices for ensuring the continuity and recoverability of their critical telecommunications services. Business continuity guidelines

identify five telecommunications-related practices that organizations can follow to improve the continuity of their critical telecommunications services: developing and maintaining an inventory of existing telecommunications services, identifying those services critical to continued operations, identifying the risks to those services, developing strategies and solutions to mitigate those risks, and testing those risk mitigation and continuity strategies.⁶ Specifically, the critical organizations we reviewed inventoried their voice and data telecommunications services and identified those services critical to their operations. The organizations also took actions to identify and mitigate their respective risks. For example, to mitigate the risk that a single failure point in their internal networks might disrupt their operations, all organizations linked their facilities to public networks at two diverse points on their premises and distributed those connections throughout their facilities through redundant cabling. To limit their exposure to disruptions in public network facilities, some organizations also subscribed to services that linked their facilities to the public network at multiple points and also linked them to services that would reroute their connections around failure points that might occur in the public networks. To improve service recoverability, six of the seven organizations were also taking advantage of a federal telecommunications priority program that would provide increased priority for restoration of the key telecommunications circuits in their inventories in the event of a disruption.⁷ These critical organizations were also testing their own abilities to recover their communications operations during a disaster and to communicate with key customers and organizations. Further, within their overall continuity strategies, most critical organizations were either establishing or continuing to operate out-of-region telecommunications facilities that would, among other things, reduce the risk that a failure in local telecommunications services at any one location would pose a risk to their continuing operations.

Finally, given that most organizations had limited resources, effectively managing operations risks involved balancing additional protections for facilities, personnel, and systems with enhancing business continuity capabilities. As part of this process, organizations take into consideration that enhancing capabilities in one area can help mitigate vulnerabilities in another area. For example, as noted previously, four of the critical

⁶The business continuity guidelines considered are described later in this report.

⁷This program is described later in this report.

organizations we reviewed had weaknesses in their physical security but also had geographically diverse backup facilities capable of conducting some or all of the organization's critical operations, mitigating the effect of a disruption at the primary facility. That is, if a physical security weakness allowed a disruption to occur at the organization's primary facility, operations could be transferred to a backup facility. Similarly, one organization that had not yet implemented a geographically diverse backup facility had made significant improvements to the physical security protections in place at its primary facility, which can help reduce the likelihood of that facility becoming incapacitated by potential physical attacks.

Broker-Dealers and Banks Also Reduced Their Risk of Disruption, but Some Faced Increased Risk Because of Concentration of Key Staff

The trading firms with whom we spoke—eight trading firms, including five large broker-dealers and three banks whose activities represent a significant portion of the total trading and clearing volume on U.S. markets—also took steps to improve their recovery capabilities, but some still faced increased risk of disruption. The smooth functioning of U.S. securities markets also depends on the ability of trading firms to conduct trading and clear and settle their transactions. In our 2003 report, we noted that because of the considerable efforts required for broker-dealers to restore operations, insufficient liquidity existed to open the markets during the week of the September 2001 attacks. For example, several large broker-dealers had not invested in backup facilities and had to recreate their trading operations at new locations; others needed to improve their business continuity capabilities for telecommunications. All of the firms we spoke with during this review said they had backup data centers capable of running critical applications and also had alternate locations out of which key staff could operate if the primary facilities should become unusable. For example, to address the potential for a region-wide disruption in New York City, one firm was developing a geographically diverse backup center. Another firm improved its ability to ensure the availability of critical staff by dividing key technical and business staff between two separate locations. All of the firms also took steps to improve their ability to retain telecommunications capabilities in the event of a disruption. For example, all five of the broker-dealers with whom we spoke had begun using the Secure Financial Transaction Infrastructure, a private telecommunications network linking financial market participants.⁸ Four of the broker-dealers

⁸This network is described in more detail later in this report.

and all three of the banks also said they were required to meet federal regulatory goals for the recovery of their clearing and settlement operations and that they were taking steps that would allow them to meet those goals within the recommended time frames.⁹

However, four of these firms were at greater risk of a disruption to their trading operations than other firms because of the concentration of key trading staff in a single location at the same time. Each of these firms did have alternate locations out of which key trading staff could work, which would allow them to recover their trading activities if their primary site were damaged or inaccessible. However, officials at these firms said that if the trading staff at the primary site were incapacitated, they would either not be able to resume trading quickly enough to meet regulators' goal of recovering trading activity on a next-day basis, or if able to resume trading, they would not be able to trade at normal capacity. For example, officials at two firms said that if they were to lose their trading operations staff, it would likely take several weeks to reconstitute their trading operations, even using staff from other locations. Officials at one of these firms said that replacing highly skilled trading staff with inexperienced staff could put the firm's capital at risk and that while they might eventually reconstitute their trading operations, they would likely exit the market for an indefinite period of time. Although officials at both of these firms said they recognized that they faced increased risk, they said at this point, the decreased efficiency and increased costs that would be associated with splitting or rotating these staff were viewed as too great, compared with the potential risk of disruption.

Securities Industry Organizations Undertook Testing and Crisis Coordination Efforts

In addition to taking actions individually, securities market participants also have worked jointly to improve the readiness of the financial sector for potential future attacks. One of the weaknesses we noted in our 2003 report was that some organizations had not completely tested their business continuity capabilities, and some also lacked sufficient connectivity to the backup sites of other organizations. To increase the industry's overall readiness, the Securities Industry Association (SIA), which represents over 600 of the broker-dealers active in U.S. markets, has been coordinating an industry-wide testing project since September 2002. The first phase of the project had broker-dealers testing connections from

⁹These guidelines are described in more detail later in this report.

their backup facilities to the core clearing and settlement organizations and correctly sending and receiving information. The second phase of the project will involve broker-dealers, exchanges, and other securities market participants in exercises that will simulate regional power and telecommunications outages. During the exercises, participants will be expected to conduct critical operations from an alternative location as well as test connectivity and communications capabilities.

Although testing took longer than originally envisioned, SIA substantially completed the first phase by June 2004. According to SIA officials, smaller firms that are not testing as quickly as others contributed to the delay. Also according to SIA staff, the more than 110 firms that completed at least part of the first phase of testing represented over 80 percent of broker-dealer trading activity, and nearly all of the 25 largest firms have completed most or all parts of this testing. Further, SIA conducted a disaster simulation exercise—involving key industry participants as well as SEC—in May 2004 to help better prepare for the second phase of testing, which was scheduled to begin in the third quarter of 2004.

To address another concern revealed by the 2001 attacks, securities market associations established crisis command centers or other coordination procedures. Just after the September 2001 attacks, some market participants encountered difficulties in communicating and coordinating with other market participants, regulators, and governmental bodies that responded to the disaster. More specifically, to coordinate the industry's response and the dissemination of information during a crisis, in June 2002 SIA created a crisis command center. SIA also placed a representative at the New York City Office of Emergency Management, an office that acts as an interagency coordinator in partnership with local, state, federal, and private entities to provide comprehensive emergency response, hazard planning and disaster mitigation to New York City. According to SIA officials, they activated the SIA command center during the August 2003 blackout and during Hurricane Isabel in September 2003, allowing them to test and validate the functioning of the command center.

In addition, the trade association that represents firms active in bond trading, the Bond Market Association, also took action to improve its members' response to future crises. According to organization officials, this association created a structure for coordinating the response of participants in the fixed-income securities markets. The association would communicate with its members through one of its standing committees regarding the condition of the fixed-income securities markets and the

potential opening and closing of those markets. In addition, the association's committee would share information and coordinate its actions with the SIA command center.

Finally, information regarding business continuity practices and potential threats to the industry has been shared with market participants. For example, SIA collected and distributed business continuity best practices to its members, established subcommittees to study business continuity-related issues, and conducted conferences to share and foster discussion of these issues in the securities industry. Also, Treasury designated another organization, the Financial Services Sector Coordinating Council (which comprises representatives from private firms in the financial industry) as the private-sector coordinator for critical infrastructure protection for the banking and finance sector. In particular this council, along with SIA and the American Bankers Association, has supported and promoted use by the financial sector of the Financial Services Information Sharing and Analysis Center (FS/ISAC), a mechanism to gather, analyze, and share information on threats, incidents, and vulnerabilities faced by the financial sector. The council also has been participating in educational and outreach efforts in conjunction with the Financial and Banking Information Infrastructure Committee, which coordinates critical infrastructure protection among federal financial regulators.

Steps Are Under Way to Meet Challenge of Improving the Resiliency of Telecommunications

The September 2001 terrorist attacks highlighted the critical importance of resilient telecommunications services for the continued operation of U.S. financial markets. The resulting damage disrupted telecommunications service to thousands of businesses and residences, and some firms learned that their services were not as robust as they believed prior to that event. Since 2001 terrorist attacks, telecommunications groups and carriers and financial market participants have worked to improve the resiliency and the recoverability of telecommunications services in the event of future disruptions.

September 2001 Attacks
Highlighted Financial Sector
Dependence on
Telecommunications
Services and Challenges of
Maintaining Diverse
Systems

As we described in our 2003 report, the 2001 terrorist attacks resulted in significant damage to telecommunications facilities, lines, and equipment. The loss of telecommunications service as well as damage to power and transportation infrastructure delayed the reopening of the markets. Much of the disruption to voice and data communications services throughout lower Manhattan—including the financial district—occurred when one of the buildings in the World Trade Center complex collapsed into an adjacent Verizon communications center at 140 West Street, which served as a major local communications hub within the public network. Approximately 34,000 businesses and residences in the surrounding area lost services.¹⁰ The loss of this facility also resulted in disruptions to customers in other service areas because other telecommunications carriers had equipment colocated in 140 West Street that linked their networks to Verizon and considerable amounts of telecommunications traffic that originated and terminated in other areas also passed through this location. AT&T's local network service in lower Manhattan was also significantly disrupted following the attacks.

The attacks also highlighted the difficulties of ensuring that the telecommunications services required to support critical financial market operations could withstand the effects of network disruptions. One of the primary ways that users of telecommunications services try to ensure that their services will not be disrupted is to use diverse telecommunications facilities to support their needs, including diversely routed lines and circuits. These steps are necessary to ensure that damage to any single point in one communications path does not cause all services to fail. However, ensuring that telecommunication service carriers actually maintain diverse telecommunications services is a long-standing financial industry concern. For example, a December 1997 report prepared by the President's National Security Telecommunications Advisory Committee (NSTAC) noted, "despite assurances about diverse networks from the

¹⁰When this Verizon facility was damaged, about 182,000 voice circuits, more than 1.6 million data circuits, and more than 11,000 lines serving Internet service providers were lost.

carriers, a consistent concern among the financial services industry was the trustworthiness of their telecommunications diversity arrangements.”¹¹

The ongoing operation and maintenance of network facilities can itself pose a challenge to ensuring diversity of services. To improve the reliability and efficiency of their networks, telecommunications carriers can change the physical network facilities they use to route circuits in a process they call “grooming.” This process can result in a loss of diversity over time, however, if diverse services are rerouted onto or through the same facilities. For example, as our 2003 report noted, many financial firms that thought they had achieved telecommunications service diversity still experienced service disruptions as a result of the September 2001 attacks. Some of these firms indicated that although they were assured that their communications circuits flowed through physically diverse paths, at the time they first acquired those services, their service providers rerouted some circuits over time without their knowledge, eliminating the assurance of diversity and leaving the firms more vulnerable to disruption.¹²

However, an NSTAC 2004 report noted that carriers would have to follow labor-intensive, manual processes to ensure route diversity and monitor that condition on an ongoing basis.¹³ NSTAC also reported that guaranteeing that circuit routes would not be changed could actually make an organization’s service less reliable because their circuits could lose the benefit of networking technologies that automatically reroute circuits in the event of facility failures.

¹¹The President’s National Security Telecommunications Advisory Committee, *Financial Services Risk Assessment Report*, (December 1997), p. 38. This committee serves as a presidential advisory group to the National Communications System, which, among other things, coordinates planning of national security and emergency preparedness communications for the federal government. NSTAC is comprised of industry officials that advise the U.S. government on policy and technical issues regarding emergency communications, information assurance, critical infrastructure protection and related concerns.

¹²GAO-03-251, p. 58 and GAO-03-414, p. 57.

¹³The President’s National Security Telecommunications Advisory Committee, *Financial Services Task Force Report*, (April 2004).

New Private Telecommunications Network Created for Financial Market Participants

Responding to the challenges of maintaining diversity, one financial market participant has acted to improve the resiliency of the telecommunications services supporting the financial industry. In January 2003, the Securities Industry Automation Corporation (SIAC) began operating its own private network, known as the Secure Financial Transaction Infrastructure (SFTI), to provide more reliable and “survivable” private communications services linking exchanges, clearing organizations, and other financial market participants.¹⁴ The information that travels on this network includes orders to buy and sell stocks on the New York and American stock exchanges as well as information needed to clear and settle these transactions.

SFTI was designed to overcome several of the challenges in attaining continual resiliency in telecommunications services. For example, to ensure redundancy and eliminate single points of failure, SFTI employs redundant equipment throughout, and carries data traffic over redundant fiber-optic rings whose routes are geographically and physically diverse. To access the network, users are required to connect to two or more of the eight SFTI access nodes located in Boston, Chicago, and the New York City metropolitan area. Therefore, if service is disrupted at one access node, service can still be obtained through an alternate node. Further, users can access SFTI in various ways, including obtaining a direct connection to the SFTI access nodes or connecting to one of four financial “extranet” service providers that operate their own telecommunications networks and also link to the SFTI access nodes.¹⁵ Some customers may choose to use a combination of both approaches.

To further enhance diversity throughout this private network, SIAC has contracted for auditable route diversity for the SFTI network. Because SIAC manages all SFTI facilities, it can also control all the grooming that takes place among the lines within the New York regional segment of this network. In addition, SIAC established a remote out-of-region network operations center that can manage network operations in the event of any disruption to its own New York area-based operations.

¹⁴SIAC is a jointly owned subsidiary of the New York Stock Exchange and the American Stock Exchange.

¹⁵A financial extranet is a private network that connect providers of financial information and transaction services (such as trading, clearing, and settlement) with members that use these services.

The financial industry has responded positively to SFTI since its implementation. For example, according to SIAC, financial industry associations, including SIA, the Bond Market Association, and the Investment Company Institute, which represents mutual funds, have all supported use of SFTI for their respective members. Moreover, NYSE, the American Stock Exchange, and the Consolidated Tape Authority, which oversees the systems that distribute stock quotes and completed trade information for the stock exchanges, expect that all of their participating member firms will be using SFTI to connect to its trading services, as of December 2004. As of June 2004, SIAC has signed up more than 600 customers for this network.

Federal and Local Actions Are Under Way to Improve Telecommunications Resiliency

Federal and local government entities have also taken steps to help the financial industry in preparing for and recovering from possible future disruptions to the telecommunications infrastructure. First, two presidential advisory committees have taken steps that may enhance the security and continuity of telecommunications services supporting the financial industry. The National Reliability and Interoperability Council (NRIC), which is a group of telecommunications carrier executives that advises the Federal Communications Commission, has identified existing and new best practices that, if implemented, could help carriers improve the security of their facilities, and improve recovery of services after attack or disruptions. NRIC addressed such matters as business continuity planning, physical security, emergency operations and response, and other operational procedures. Further, NSTAC, which had also studied diversity issues, recommended that the federal government support research and development activities on resiliency, diversity, and alternative technologies.

Additionally, the federal government sought to increase financial industry participation in federal programs that could enhance the recoverability of disrupted services. Specifically, the Department of Homeland Security's (DHS) National Communications System (NCS) promoted participation in its Telecommunications Service Priority (TSP) program. TSP allows financial market participants to register their key telecommunications circuits for priority restoration in the event of a crisis.¹⁶ Financial market

¹⁶TSP is used to ensure that organizations that conduct activities important for national security or emergency preparedness receive priority treatment in their use of telecommunications services that can be vital to coordinating and responding to crises. These circuits are then eligible for priority restoration in a disaster.

participants are sponsored for registration in this program by their regulatory agency. According to NCS officials, the financial industry has made greater use of the TSP program, as there are now about 4,100 financial organization circuits registered in TSP for priority restoration; more than 3,500 of those were registered since June 2002. Further, to improve the recoverability of SFTI, the Federal Reserve worked with SIAC to ensure that all SFTI access lines were registered for TSP priority restoration as those circuits were installed.

Federal financial regulators also have been working with carriers to more closely examine the diversity challenge and identify potential management solutions. In a recently initiated pilot project, the Federal Reserve has been working with the Alliance for Telecommunications Industry Solutions to examine the diversity of circuits supporting Federal Reserve networks.¹⁷ The project's goal is to develop an efficient, affordable way to document and maintain routing diversity using those circuits as a baseline. According to Federal Reserve and Treasury officials, this exercise could yield a model approach for achieving assured diversity, improve the processes required to do so, and provide a better understanding of the associated costs.

Finally, New York City officials have enhanced their ability to monitor and coordinate infrastructure recovery efforts with local carriers. City officials recently revised their Mutual Aid Restoration Consortium (MARC) agreement, which governs monitoring and coordination of restoration actions between telecommunications carriers and city officials in the event of service outages. City officials invoked this agreement in the aftermath of the September 2001 attacks to ensure that essential city government offices and operations would have adequate telecommunications service and to aid coordination of infrastructure recovery efforts by carriers operating in the city. More recently, the MARC agreement proved effective during the August 2003 blackout, in which teleconferences were used to identify and communicate urgent diesel fuel needs of carriers and to coordinate other critical assistance to share power generators and network facilities. Lessons learned from such incidents have been addressed in the revised MARC agreement.

¹⁷ATIS is an association of telecommunications industry professionals that develops technical and operations standards and solutions for the communications and related information technologies industries.

Telecommunications Carriers Are Also Taking Action to Improve Infrastructure Resiliency

Telecommunications carriers are also acting to improve the resiliency of their networks. First, those carriers rebuilding facilities that were damaged or lost in the attacks have been replacing these facilities with designs that provide greater diversity to their infrastructure in lower Manhattan. For example, to avoid single points of failure in its network, Verizon redesigned its network to minimize circuits that only pass through a switching facility on their way to other termination points. This should reduce the potential for service in one area to be lost when damage occurs to facilities in other areas. In addition, Verizon has also used more resilient and physically diverse fiber optic systems within lower Manhattan, which also may provide alternate network access capabilities at strategic locations. Similarly, as part of its own restoration effort, AT&T officials said they rebuilt two central office facilities at more geographically diverse locations and upgraded their fiber-optic networks.

Telecommunication carriers also reported that they were improving their own business continuity plans to better ensure their ability to recover after a disaster. For example, officials at both Verizon and MCI said they had reexamined their continuity plans and developed new recovery strategies to improve their continuity capabilities. In addition, officials at AT&T informed us that they were continuing to conduct quarterly network disaster recovery tests at different locations throughout the United States that simulate the recovery of damaged switching facilities.

Finally, telecommunications carriers have tried to increase telecommunications resiliency by offering additional services to their customers, including financial market participants. As we described in our 2003 report, carriers offer various services that can improve the reliability and recoverability of existing telecommunications.¹⁸ For example, carriers offer fiber-optic networks to provide more reliable access to public networks; services to redirect their switched telecommunications services, such as voice calls, to another business location; and alternative network connectivity solutions such as high bandwidth, point-to-point radio connectivity to another location or network node.

¹⁸GAO-03-251, p. 103 and GAO-03-414, p. 102.

Federal Financial Regulators Took Actions to Improve the Readiness of Securities Markets, but Further Actions Needed

Since our 2003 report, federal financial regulators, including SEC, have identified vulnerabilities, participated in tests and exercises, and developed recovery goals and business continuity guidelines to improve the preparedness of securities markets for terrorist attacks and other disasters. For example, banking and securities regulators have issued joint guidance providing recovery goals for market participants that perform critical clearance and settlement activities. Partly in response to a recommendation in our 2003 report, SEC also has issued guidance providing goals for trading activities to resume on securities exchanges. However, SEC has not developed a complete assessment of securities markets readiness to resume trading after major disruptions, which increases the risk that the reopening of the markets could be delayed.

Financial Regulators Participated in Exercises, Information Sharing, and Conducting Examinations of Financial Sector Readiness

Since our 2003 report, federal financial regulators have participated in exercises that assess readiness for potential disasters. For example, Treasury, the Federal Reserve, SEC, and the Commodity Futures Trading Commission have taken part in several disaster recovery exercises sponsored by DHS, including the TOPOFF exercises, which simulated physical attacks, and the Livewire exercise, which simulated a cyber attack. In addition, as part of the Financial and Banking Information Infrastructure Committee, the federal financial regulators have conducted an analysis of financial sector vulnerabilities, including those involving dependencies on other critical infrastructures, such as telecommunications and power.

Financial regulators have also been involved in various information sharing efforts. For example, Treasury has also supported and promoted the FS/ISAC, which as described earlier gathers, analyzes, and shares information on threats, incidents, and vulnerabilities faced by the financial sector. In 2004, Treasury provided additional funding to FS/ISAC to allow it, among other things, to expand its membership and services to even the smallest financial institutions, such as community banks. Treasury has also been involved, along with the Federal Deposit Insurance Corporation, in conducting educational outreach events in various cities on sound business continuity practices. Treasury is also working with DHS to continue developing “Chicago First,” an emergency preparedness program designed to coordinate activities among financial sector participants and federal, state, and local government officials. Treasury is promoting this program as a model for other cities to implement.

Banking and securities regulators have also taken steps since our 2003 report to assess the efforts of banks and securities firms to withstand and recover from disasters. For instance, in March 2003 the Federal Financial Institutions Examination Council (FFIEC), which issues joint regulatory and examination guidance used by financial regulators in overseeing financial institution such as banks and credit unions, issued a Business Continuity Planning Booklet that provided updated guidance and examination procedures on this topic.¹⁹ In the booklet, FFIEC requires depository institutions to develop business continuity plans that will effectively minimize service disruptions and financial loss, test the plans at least annually, and subject the plans to independent audit and review. In addition, it asks institutions to consider in their planning the potential for wide-area disasters and the resulting loss or inaccessibility of staff, as well as the extent to which their institution is dependent upon other financial system participants and service providers. According to one financial regulator responsible for conducting examinations based on these guidelines, an informal analysis showed that larger financial institutions were doing better than smaller ones in meeting the guidelines. As a result, officials at that regulator said they had begun developing guidance to help smaller institutions better meet the business continuity guidelines.

SEC has also conducted examinations of broker-dealers that included reviews of information security and business continuity efforts. For example, SEC's Office of Compliance Inspections and Examinations (OCIE) administers SEC's inspection program for broker-dealers, including monitoring broker-dealers' compliance with Regulation SP, which deals with the privacy of consumer financial information.²⁰ As part of their review of broker-dealers' ability to protect consumer information, OCIE staff review those organizations' information security capabilities. In addition, since our 2003 report, OCIE has begun incorporating into its broker-dealer examinations the business continuity practices presented by federal financial regulators in an interagency paper (described in the following paragraph).

¹⁹FFIEC comprises officials from the Federal Reserve, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision. The booklet rescinds and replaces chapter 10 of the *1996 Information Systems Examination Handbook, Corporate Contingency Planning*.

²⁰17 C.F.R. 248.

Financial Regulators Developed Business Continuity Guidelines for Clearing and Settlement

Federal financial regulators also have jointly focused on continuity issues to reduce the risk of disruption for the financial markets from terrorist attacks or other disasters. In April of 2003, securities and banking regulators issued the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*.²¹ Issued by SEC, the Federal Reserve, and the OCC, this interagency paper identifies business continuity practices that core clearing and settlement organizations and firms that play a significant clearing or settlement role in critical financial markets are expected to follow. Core organizations include clearing organizations responsible for securities and other financial products and payment system processors. In addition to these organizations, the interagency paper also applies to financial institutions, including banks and broker-dealers, which conduct significant amounts of trading and clearing activities. If these firms were unable clear and settle the outstanding trades that they or their customers conducted, they could create payment problems for other participants in the markets.²² By proposing that these organizations and firms follow the practices identified in the interagency paper, regulators expect to minimize the immediate systemic effects of a wide-scale disruption—by setting goals for key payment and settlement systems to resume operation promptly following a wide-scale disaster, and for major participants in those systems to recover sufficiently to complete pending transactions.

In the interagency paper, the regulators outline various practices for organizations and firms to follow and set goals related to resumption of their clearing and settlement activities. First, these organizations and firms are expected to identify the clearing and settlement activities that they

²¹The Board of Governors of the Federal Reserve, the Office of the Comptroller of the Currency, and Securities and Exchange Commission, *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, (Washington, D.C.: April 2003).

²²Specifically, the interagency paper defines core clearing and settlement organizations as either (1) market utilities, such as government-sponsored services or industry-owned organizations, whose primary purpose is to clear and settle transactions for critical markets or transfer large-value wholesale payments; or (2) private-sector firms that provide clearing and settlement services that are integral to a critical market. The paper defines significant firms as those that participate (on their own behalf or for their customers) with sufficient market share in one or more critical financial markets that their failure to settle their own or their customers' material or pending transactions by the end of the day could present systemic risk. Firms are generally considered significant in a particular critical market if they consistently clear or settle at least 5 percent of the value of transactions in that market.

perform in support of critical financial markets. They are also expected to determine appropriate recovery and resumption objectives for those activities. The regulators state that, at minimum, the organizations and firms are expected to be able to recover within the same business day.²³ To realistically achieve this, the regulators expect that these organizations and firms would maintain geographically dispersed resources to meet their recovery and resumption objectives. Specifically to be consistent with best practices, backup facilities for clearing functions should be as far away from the primary facility as necessary to avoid being subject to the same set of risks as the primary facility. The backup facilities also should not rely on the same infrastructure—such as power and telecommunications—as the primary facility, and the operation of the backup facility should not be impaired by a wide-scale evacuation at, or the inaccessibility of staff that service, the primary site. In addition, the regulators expect that the organizations and firms would engage in routine use or testing of their recovery and resumption arrangements.

The regulators also included deadlines for achieving continuity goals in the interagency paper. For example, core clearing and settlement organizations are expected to implement the practices the paper advocates, by the end of 2004. Significant banks and broker-dealers are expected to have implemented such practices by April 2006. According to banking and securities regulatory officials, they are monitoring the progress that organizations and firms are making in meeting these deadlines.²⁴

SEC Set Business Continuity Goals for Securities Trading

SEC also has provided recovery goals and business continuity best practices to exchanges and ECNs that conduct securities trading in the United States. In our 2003 report, we recommended that SEC work with the

²³To ensure that they can meet the goal of recovering within the same business day, the paper notes that core organizations should strive to be able to recover within 2 hours of a disruption, with significant firms striving to be able to recover within 4 hours.

²⁴In another clearing-related effort, the Federal Reserve, along with representatives from clearing banks, securities dealers, trade associations, and others formed the Working Group on Government Securities Clearance and Settlement. Tasked with assessing alternatives for reducing the vulnerability stemming from concentration among clearing banks for government securities, this group has proposed that a new legal entity could assume the operations if one of the clearing banks was unable to operate as the result of financial or legal difficulties. However, this proposal, called the NewBank plan, is not intended to address operational disruptions and assumes the staff, systems, and data of the affected clearing bank remain intact.

industry to develop such goals and sound business continuity practices and identify organizations that should follow them. In September 2003, SEC issued a policy statement that establishes business continuity principles to be followed by the organizations that execute trades in securities, including the NYSE, the Nasdaq Stock Market, Inc. (NASDAQ), the regional stock exchanges, the options exchanges, and ECNs, which match buy and sell orders for securities.²⁵ The business continuity principles SEC published include

- establishing a business continuity plan that anticipates the resumption of trading no later than the next business day following a wide-scale disruption;
- maintaining geographic diversity between primary and backup sites;
- ensuring the full resiliency of important shared information systems, such as market data collection and dissemination systems; and
- testing the effectiveness of backup arrangements in recovering from wide-scale disruptions.

SEC expects the securities markets and ECNs to implement business continuity plans reflecting these principles, no later than the end of 2004. According to SEC staff, they are monitoring the progress of the exchanges and ECNs in implementing the policy statement through their examinations of these organizations.

In addition to establishing recovery goals, SEC has taken additional actions to ensure that sufficient venues for trading would likely be available after a major disaster. As we noted in our 2003 report, SEC staff have asked NYSE and NASDAQ to be prepared to trade the other's securities should one trading floor go down. Officials at both of these markets said they have made the necessary system changes and have tested their members' ability to trade the other markets' securities. SEC officials said that they assessed had the ability of these two organizations to provide such backup and were confident that these markets had the necessary capacity and systems to do so. If neither NYSE nor NASDAQ is able to resume trading, ECNs and regional exchanges would have to assume the trading of the stocks that are

²⁵U.S. Securities and Exchange Commission, *Policy Statement: Business Continuity Practices for Trading Markets* (Washington, D.C.: September 2003).

normally traded on those markets. SEC staff said that, based on discussions with ECN officials and information obtained from inspections of these entities, collectively, the ECNs and regional exchanges have sufficient capacity to take on significant additional amounts of trading volume that would result from such an event. Although none of the organizations involved—NYSE, NASDAQ, ECNs, and regional exchanges—are required to assume such additional trading activity, according to SEC staff these organizations all have a strong business incentive and competitive motivation to do so.

Finally, SEC approved business continuity goals for the broker-dealers that conduct trading in U.S. securities markets. In April 2004, SEC approved essentially identical rules from NASD and NYSE that require their members to develop business continuity plans.²⁶ According to these rules, the broker-dealer members of these organizations must develop business continuity plans that address various elements, including

- data backup and recovery,
- alternate means of communication with customers,
- alternate physical locations for employees, and
- consideration of the impacts to critical customers and counterparties.

These rules do not require trading firms to actually have plans to resume operating or trading activities after a disaster. Instead, if a disaster occurred and broker-dealers were unable to continue operating, the rules require broker-dealers to develop procedures to ensure that they promptly could provide customers with access to their funds and securities if the broker-dealers were unable to continue business operations. These rules appear to respond to our 2003 recommendation that SEC work with the securities industry to develop business continuity guidelines that, at a minimum, require broker-dealers to allow customers to readily access their cash and securities. NYSE expected its members to implement its rule by August 5, 2004, and NASD expected implementation by September 10, 2004.

²⁶NYSE Rule 446 and NASD Rule 3510.

SEC Has Not Fully Analyzed Capabilities of Trading Firms to Resume Operations

Although the actions securities and banking regulators have taken will likely improve the preparedness of the securities markets to withstand future disruptions, SEC has not conducted the comprehensive assessments that would allow it to better ensure that trading in the securities markets could promptly resume following a wide-scale disaster. Preparing for trading activities to 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. Furthermore, as previously noted, financial regulators expect markets to resume both clearing and trading activities within 1 business day or less. In addition, according to Treasury staff responsible for its critical infrastructure protection program, ensuring that markets are not closed for lengthy periods is important to maintaining investor confidence during the uncertainty that accompanies major disasters.

SEC officials said that if the organizations and firms expected to adhere to the guidance and best practices in the interagency paper and SEC's policy statement did so, U.S. securities markets would be able to recover even from an attack or disaster that resulted in wide-scale damage or disruption. However, SEC officials explained that they do not have specific authority to require broker-dealers to participate in the markets to any degree and neither the interagency paper on clearing and settlement, the SEC policy statement, nor the NYSE and NASD business continuity rules currently require individual broker-dealers to be prepared to resume their trading operations following a disaster.

Although the ability to resume trading will also depend on whether sufficient numbers of trading firms are willing and able to resume operations, concerns persist over the potential readiness and the threat of disruption to these firms. As we discussed in our 2003 report, part of the delay in reopening the trading markets after the September 2001 attacks was attributable to the difficulties that some broker-dealers faced in recovering their trading operations. As we noted previously in this report, some of the key trading firms continue to face increased risk that their operations would be disrupted and acknowledged that they may not be able to resume trading in some cases. Furthermore, in August 2004, DHS announced that intelligence had been received that terrorists may have targeted the facilities of individual U.S. banks and broker-dealers as well as other financial related entities for potential attacks.

Although SEC had taken some steps to assess broker-dealer readiness, it had not done a systematic analysis to determine whether sufficient

numbers of firms would be capable of resuming trading within regulators' current expectations. SEC staff said they were aware of this risk and had done some informal assessments of where major broker-dealer facilities are located. The staff also noted that some firms could likely use staff located elsewhere in the country or in foreign locations to trade on U.S. markets. However, officials at some of the key firms we contacted indicated that they did not always have sufficient numbers of trained staff elsewhere who could assume their U.S. trading activities. One of the officials told us in June 2004 that SEC would begin evaluating broker-dealers' trading staff arrangements and, where appropriate, ask firms to voluntarily address the risk posed by having their trading staff in single locations in the same geographic area as other such organizations. One of the officials said that SEC did not yet have a time frame in which firms would complete such actions and acknowledged that such organizations could have valid business reasons for not taking those actions. For example, relocating trading staff or spreading them across more than one location can be expensive and reduce the efficiency of a firm's operations.

SEC officials also told us that if a wide-scale disaster disrupted trading at a number of broker-dealers in one geographic area, firms outside that area could step in and conduct trading. Such firms could include the regional broker-dealers located around the country. However, SEC staff had not conducted a full analysis of the number of firms, where they are located, or the amount of trading volume they normally handle. These firms also would need sufficient staffing and financial resources to support increased trading volumes.

SEC Took Some Actions to Enhance Its ARP Program but Has Not Addressed Other Limitation to Its Effectiveness

Since our 2003 report, SEC has acted to improve the ARP program, but has not addressed other long-standing issues that hamper the effectiveness of the program and hinder SEC's oversight. These issues include insufficient resources with the appropriate expertise to increase the frequency, depth, and comprehensiveness of its examinations and the lack of a rule that mandates compliance with the ARP program's tenets and examination recommendations. The ARP program also appears to have limitations in its ability to oversee information security issues. Given the limitations that affected the ARP program over time, continued assessment of whether the ARP program's placement within SEC's organizational structure might identify options that could better assure that it receives the appropriate resources to perform its important mission.

SEC Created ARP to Oversee How Exchanges, Clearing Organizations, and ECNs Addressed Operations Risks

SEC created the ARP program in 1989 in response to operational problems that markets experienced during the 1980s at exchanges, and clearing organizations, and later, ECNs. The program addresses operations risk issues at these entities, including physical and information security and business continuity. SEC did not create rules for these entities to follow but instead issued two ARP statements that provided best practices in various information technology and operational areas with which the exchanges and clearing organizations would be expected to comply voluntarily. As part of the ARP program, these entities (among them, some of the critical organizations we reviewed for this report) are expected to have the relevant aspects of their operations reviewed periodically by independent reviewers, which can include the entities' own internal auditors or external organizations, such as accounting firms or information security consultants. In addition, SEC's ARP staff conduct periodic on-site reviews of these organizations to assess selected information technology or operational issues and make recommendations for improvements when necessary. During any examination, ARP program staff analyze the risks faced by each entity to determine which are the most important to review. As a result, ARP staff are not expected to review every issue specific to an entity during each examination.

SEC Has Taken Steps to Improve ARP Program

SEC staff said they have made improvements to the ARP program. SEC officials said they have placed more emphasis on monitoring the status of the recommendations made as result of ARP reviews, with the result that they can better determine whether entities within the program implement the recommendations. ARP staff meet quarterly with ARP management to review the status of and progress on any outstanding ARP recommendations. As a result, ARP staff have more frequent contact with the entities they examine to obtain information about the status of recommended actions. According to these officials, this more frequent follow-up lets the exchanges, clearing organizations, and ECNs know that they cannot let action on recommendations wait until the next ARP review, which can be several years away. ARP officials said that as a result of these efforts, they have been able to close outstanding recommendations and indicated that the level of cooperation they receive from the entities has improved.

SEC staff also said that a recent reorganization within its Division of Market Regulation also improved program effectiveness. According to SEC staff, in November 2003, SEC merged ARP program staff with other

Division of Market Regulation staff that conducted surveillance of trading in the markets using information systems. While remaining within the Division of Market Regulation, this combined group is now called the Office of Market Continuity. Although the merger only marginally increased the number of staff allocated to the ARP program (from 10 to 11 staff and a new Assistant Director), SEC staff said the merger gave them access to some additional staff resources and also increased the visibility of the ARP program within SEC. These additional staff are not examiners but can be used to draft letters and research legal issues.

SEC Has Not Addressed Long-standing ARP Program Limitations

Although it has taken some actions to improve the ARP program, SEC still has not addressed weaknesses that have hampered the effectiveness of the program, such as making ARP a rule-based program and improving ARP's staffing resources and expertise. As we reported in 2001 and 2003, the entities subject to the ARP program had not always implemented or addressed significant ARP staff recommendations, including some related to inadequate backup facilities, security weaknesses, and inadequate information system processing capacity.²⁷ Some of these unaddressed weaknesses later led to problems. For example, one organization experienced problems related to ensuring adequate processing capacity that delayed the implementation of decimal pricing by all securities markets for 3 months. In another instance, SEC staff raised concerns about the lack of a backup operating facility at an entity that had its primary facility in the area that would later be affected by the 2001 terrorist attacks. In some cases, organizations subject to ARP were also not providing the reports of system changes and other events that SEC expects to receive under the program. To address this issue, we recommended in our 2003 reports that SEC issue a rule that would make adherence to tenets of the ARP program and the recommendations of its staff mandatory for exchanges and clearing organizations. In contrast, ECNs have had to comply with ARP recommendations since 1998, when SEC adopted a rule increasing regulatory scrutiny of alternative trading systems.²⁸ SEC's Inspector General has also expressed similar concerns about compliance with ARP program recommendations. SEC officials said they drafted a rule making exchange and clearing organization compliance with ARP tenets

²⁷GAO-01-863, GAO-03-251, and GAO-03-414.

²⁸Securities and Exchange Commission, Final Rule: Regulation of Exchanges and Alternative Trading Systems, Release No. 34-40760 (Dec. 8, 1998).

mandatory but had not yet submitted it for review by the SEC Commissioners. SEC staff told us that the level of cooperation with recommendations and other expectations that they have received from the entities subject to the ARP program has improved since the 2001 terrorist attacks. However, they acknowledged that without a rule SEC lacks greater assurance that these organizations will continue to comply with ARP recommendations, particularly key recommendations that could be costly for the entities.

SEC also has not fully addressed the adequacy of resources dedicated to the ARP program, another long-standing issue. Our 2001 and 2003 reports described how a lack of resources hampered the ability of the ARP program to oversee the operations of the entities it reviews.²⁹ For example we reported that these resource constraints affected the ARP program's ability to conduct frequent examinations. In our 2003 report, we reported that the intervals between ARP examinations had exceeded 3 years for five of the seven critical financial market organizations that we reviewed, with the other two organizations not being reviewed for 6 years or more. According to SEC staff, they have developed a tiered examination schedule for the organizations subject to ARP. Under this schedule, first-tier organizations, including the clearing organizations and most active markets, are to be reviewed annually. Second-tier organizations are reviewed based on their risk assessment profile under a 3-year inspection cycle, and third-tier firms, such as small ECNs are inspected for cause. The SEC staff said they have met this schedule thus far.

As a result of these concerns, we recommended in 2003 that SEC expand the level of staffing and resources devoted to ARP if sufficient funds were available. Although in recent years, SEC's overall resources have significantly increased—its funding increased 45 percent in 2003—as of May 2004, no significant additional resources had been allocated to the ARP program. SEC staff said the recent creation of the Office of Market Continuity provided them with access to some additional staff resources, as noted earlier, but demands on ARP staff also have grown. For example, in our 2003 report, we noted that ARP staff workload had expanded to cover entities with more complex technology and communications networks. As entities continue to implement new technologies and networks, ARP staff workload is likely to increase further. In August 2004,

²⁹GAO-01-863, GAO-03-251, and GAO-03-414.

staff in SEC's Market Regulation Division said they will ask for additional staffing for the ARP program.

The ARP program's ability to obtain and retain staff with sufficient technical skills has also been an issue in the past and may have affected its ability to effectively oversee information security issues at the entities it oversees. In previous reports, we have described difficulties SEC has had in retaining qualified and experienced staff in its ARP program, as well as concerns of industry officials over ARP staff expertise.³⁰ During this review we identified examples where ARP staff could benefit from additional technical expertise. For example, reviews by internal and external reviewers are a key component of the ARP program and SEC officials said they attempt to track all significant issues and recommendations to ensure they are addressed. However, we found that internal and external reviewers at some of the critical organizations we reviewed had identified important actions to improve the security of their information systems, but that the organizations had not implemented them. In addition, at some of the critical organizations, we identified important additional opportunities for improvements in information security that had not been previously identified by internal or external reviewers or by SEC's ARP staff.

One way organizations can help ensure that their various functions receive the appropriate level of resources, including staff and expertise, is to ensure that those functions are properly aligned within the organization's overall structure. Currently, the ARP program is located within the Division of Market Regulation and, as such, is a small part of a larger division whose primary responsibility is to establish and maintain standards for the operation of fair, orderly, and efficient markets. As noted previously, SEC recently relocated the ARP program within the Division of Market Regulation, and SEC officials told us that this move has been beneficial and that they continue to assess the impact of the reorganization on the program's effectiveness. However this move has not yet resulted in significant additional staffing or additional technical expertise specifically dedicated to the ARP program. Other possible placements that might prove beneficial for the ARP program from a resource and expertise standpoint could include placing the ARP program with the other examination staff within SEC's Office of Compliance Inspections and Examinations, or combining its staff with those having similar technical expertise within

³⁰See GAO, *SEC Operations: Increased Workload Creates Challenges*, GAO-02-302 (Washington, D.C.: Mar. 5, 2002), GAO-01-863, GAO-03-251, and GAO-03-414.

SEC's Office of Information Technology. Realigning the ARP program within SEC could, however, have potential disadvantages. For example, having ARP staff within the Division of Market Regulation, as it is now, provides valuable expertise and information gathering abilities and allows this examination function to be linked with the related policy-making function.

Conclusions

The securities market organizations we reviewed all had reduced the risk that their operations would be disrupted by terrorist attacks or other disasters. In addition, financial market participants and telecommunications organizations increased the resiliency of the critical telecommunications services necessary for the functioning of the markets. Further, financial regulators have issued guidance to these organizations that, if implemented, should greatly increase the ability of the markets to recover. However, as of May 2004, a number of the critical financial market organizations and the broker-dealers and banks that conduct significant trading activities remained at a greater risk of disruption than others from a wide-scale event because they lacked certain business continuity capabilities. The ability of U.S. financial markets to recover and resume operating in the wake of any future attacks or disasters depends upon the extent to which these critical market participants augment their business continuity capabilities or mitigate existing weaknesses.

One of the lessons learned from the September 2001 attacks was that without key broker-dealers able to trade, the markets could not reopen. As we noted in our 2003 report, insufficient liquidity existed to open the markets during the week of the September 2001 attacks because of the considerable efforts required for broker-dealers to restore operations. However, SEC currently lacks adequate assurance that the actions of organizations that trade in the markets will be sufficient to ensure that this important activity can also resume. Although joint regulatory guidance addresses organizations' clearing and settlement activities, and SEC's own policy statement directs exchanges and ECNs to implement sound business continuity practices, the firms that conduct trading activities in U.S. markets are not similarly required to implement such practices, and SEC officials said they do not have specific authority to require broker-dealers to participate in the markets to any degree. Nevertheless, SEC has not fully assessed whether or not sufficient numbers of firms with staff capable of trading securities would be ready to operate after a wide-scale disaster. Similarly, although many other trading firms exist, including regional firms with sizeable operations located throughout the United States, SEC has not

sufficiently analyzed the willingness and capabilities of these firms to step up and become the significant providers of liquidity necessary for fair and orderly trading to occur in the aftermath of a disaster. Once it conducts a more complete analysis of the likely readiness of trading firms to resume trading, SEC could use the results to identify actions that specific exchanges, clearing organizations, or trading firms could take to increase the likelihood that trading in the markets could resume when appropriate. Given that some disaster and damage impact scenarios are more or less likely than others, having SEC weigh the feasibility and costliness of any actions that it identifies against the potential benefits and likelihood of such scenarios occurring appears warranted.

While SEC has made some enhancements to the ARP program, it has also not made key improvements, including those we recommended in our 2003 report, that could better ensure that it is as credible and as effective as possible. Given the importance of the work with which SEC's ARP staff are tasked, ensuring that they have a specific rule to mandate compliance with ARP program tenets and sufficient staff to conduct their oversight appears justified. While SEC has made progress in ensuring that exchanges and clearing organizations implement ARP staff recommendations, such current voluntary cooperation may not always exist in the future, especially when ARP-recommended actions would be costly to an organization. The limited resources that SEC has devoted to ARP thus far have generally prevented it from conducting more frequent examinations and do not appear to have provided it with sufficient technical expertise to address important information security issues.

While the ARP program was realigned within the Division of Market Regulation in November 2003 and SEC staff indicated that they are assessing the impact on the program's effectiveness, it is not yet clear whether this change will improve the program's ability to obtain sufficient additional resources and staff with the necessary expertise. Given that the functioning of the markets is critical to our nation's economy, taking steps to better ensure that the program used to oversee operational and information security issues at these entities has sound legal authority and adequate resources and expertise is warranted at this time. Such steps would include assessing whether the placement of the program within SEC's organizational structure is optimal for ensuring that it has adequate resources and staff expertise.

Recommendations for Executive Action

To provide greater assurance that the critical trading that is conducted in U.S. financial markets can resume, in as timely a manner as appropriate, after disruptions, we recommend that the Chairman, SEC, fully analyze the readiness of the securities markets to recover from major disruptions and work with industry and other federal agencies, as appropriate, to determine reasonable actions that would increase the likelihood that trading in the markets could resume when appropriate.

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

- Establish a definite time frame for the submission of a rule requiring exchanges and clearing organizations to engage in activities consistent with the operational practices and other tenets of the ARP program;
- Assess the adequacy of ARP staffing in terms of positions and technical skill levels, including information security expertise, given its mission and workload; and
- Continue to assess the organizational alignment of the ARP program within SEC.

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 II and III, respectively. The Federal Reserve, OCC, and SEC also provided technical comments, which we incorporated in the report as appropriate.

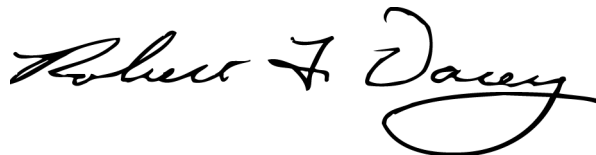
SEC generally agreed with the report and its recommendations. The letter from SEC's Chairman noted that SEC has been working actively with the trading markets, core clearing organizations, and major market participants to strengthen the resiliency of the financial markets. In addition, SEC's letter noted that it would be taking specific actions in response to our recommendations, including conducting an assessment of key broker-dealers' trading staff arrangements and the preparations of these firms to resume trading operations following a disaster. SEC also indicated that its Market Regulation Division is developing a proposed rule that would require exchanges and clearing organizations to engage in

activities consistent with the operational practices and other tenets of the ARP program and that this should be submitted to the Commission during the first half of 2005. SEC stated that it is also currently assessing the adequacy of staffing and technical skill levels within the ARP program and that increased education for its staff, hiring new staff, and engaging consultants are all ways that it could use to address its needs in this area. Finally, SEC noted that as part of the agency's routine strategic planning effort, it will continue to assess the organizational alignment of the ARP program within SEC. In its letter, the Federal Reserve noted that addressing the risks posed by the September 11 attacks continues to be a priority for the organization and that it is continuing efforts to improve the resiliency of the financial system.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees; the Secretary, Treasury; the Chairman, SEC; the Chairman, Federal Reserve; and the Comptroller of the Currency; and others who request them. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.



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



Robert F. Dacey
Director, Information Security Issues

Linda D Koontz

Linda Koontz
Director, Information Management

A handwritten signature in black ink, appearing to read 'Keith Rhodes', written in a cursive style.

Keith Rhodes
Chief Technologist
Director, Center for Technology
and Engineering

Objectives, Scope, and Methodology

The objective of this report is to describe the progress that financial markets participants and regulators have made since our 2003 report in reducing the likelihood that terrorist attacks and other disasters would disrupt market operations. Specifically, we assessed (1) actions that critical securities market organizations and key market participants undertook to reduce their vulnerabilities to physical or electronic attacks and to improve their business continuity capabilities; (2) steps that financial market participants, telecommunications industry organizations, and others took to improve the resiliency of telecommunications systems and infrastructure; (3) financial regulators' efforts to ensure the resiliency of the financial markets; and (4) the progress the Securities and Exchange Commission (SEC) has made in improving its Automation Review Policy program, which oversees security and operations issues at exchanges, clearing organizations, and electronic communications networks (ECN). As in our previous report, for purposes of our analysis we selected seven organizations whose ability to operate is critical to the overall functioning of the financial 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 security and the confidentiality of their proprietary information, we agreed with these organizations that we would not discuss their efforts to address physical and information security risks and ensure business continuity in a way that could identify them.

To assess actions that critical securities market organizations took to reduce their vulnerabilities to physical or electronic attacks and to improve their business continuity capabilities, we visited their facilities, reviewed relevant business continuity policies, and interviewed officials at the organizations. Specifically, to determine what steps these seven organizations were taking to reduce the risks to their operations from physical attacks, we conducted on-site "walkthroughs" of their 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 with 52 standards developed by the Department of Justice for federal buildings. Based on these standards, we evaluated the 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 identify types of tests an organization can perform to monitor the effectiveness of physical security measures in place, we reviewed publications and guidance, such as that

contained in our *Executive Guide on Information Security Management*¹ and obtained information from security experts within our office, including Office of Special Investigations. We obtained information on the types and extent of physical security testing performed by the organizations at their primary locations and compared it with the information we collected. We also reviewed publications and guidance, such as those issued by the Centers for Disease Control and Prevention, Federal Emergency Management Administration, and Lawrence Berkeley National Laboratory, to identify high-level countermeasures that an organization could take to mitigate the CBR threat. For each primary facility, through interviews with the organizations' security officials, we identified and compared their actions against our listing of countermeasures.

To determine what steps these seven 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 compared their information security measures with those recommended for federal organizations in the Federal Information System Controls Audit Manual, other federal guidelines and standards, and various industry electronic security best practice principles. 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 how they 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 seven 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 visited their facilities. We reviewed their BCPs and assessed them against practices recommended for financial organizations, including bank regulatory guidance. 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

¹GAO *Executive Guide on Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68, May 1998.

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 did not directly observe the operation of these backup sites, but relied on documentation, including backup facility test results, provided by the organizations. We also discussed the business continuity capabilities and improvements made by eight large broker dealers and banks that collectively represented a significant portion of trading and clearing volume on U.S. securities markets.

To determine the extent to which critical financial market organizations reduced the likelihood that their operations might be disrupted by future disasters, we also examined the telecommunications continuity practices they were following. To identify sound telecommunications-related continuity practices, we first reviewed business continuity planning guidance published by the Business Continuity Institute, the Federal Financial Institutions Examination Council, and other continuity planning guidance. Based on our review of those materials, we identified five principal practices that organizations should follow to plan for the availability of telecommunications services that are important to their continuing operations. We also discussed our selection of practices for use as criteria with a private-sector business continuity expert to affirm that our selection of these five practices was an appropriate judgment. We then examined the extent to which the critical organizations followed these practices by reviewing network documentation, continuity plans, and testing reports where available, and discussed with organization telecommunications managers their network continuity strategies and the practices they followed to mitigate perceived continuity risks. We assessed those strategies, practices, and related documentation against the five practices we identified.

To determine how financial and telecommunications industry organizations, federal and local government entities, and supporting telecommunications service providers further improved telecommunications service resiliency, including improved infrastructure diversity and recoverability, we reviewed reports and related documentation prepared by three Presidential Advisory Committees—the National Infrastructure Advisory Council, the National Security Telecommunications Advisory Council, and the Network Reliability and Interoperability Council. These reports and documentation evaluated infrastructure interdependencies and network diversity challenges, and they identified practices that telecommunications carriers and large

organizations might follow to better prepare for and recover from future network disruptions. We also reviewed plans and documentation developed by a critical financial organization to implement and operate a private network for the benefit of financial market participants. In addition, we met with managers at the Board of Governors of the Federal Reserve (the Federal Reserve) and the federal National Communications System to obtain data on the use of federal national security/emergency preparedness programs by the financial industry to improve the recoverability of important telecommunications services. We also met with New York City officials to review the status of their efforts to reestablish an agreement to coordinate and monitor the recovery of local infrastructure in the event of future service outages. Finally, we met with managers at three large telecommunications carriers to review how they were rebuilding local infrastructure in New York City, and steps taken to review and revise their own continuity plans.

To assess financial regulators' efforts to ensure the resiliency of the financial markets, including the progress SEC has made in improving its program for overseeing security and operations issues at exchanges, clearing organizations, and ECNs, we reviewed relevant regulations and interviewed officials at SEC, the Federal Reserve, Office of the Comptroller of the Currency, and the Department of Treasury. 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.

For our reviews, we relied on documentation and descriptions provided by market participants and regulators and reviews conducted by other organizations. When feasible, we also directly observed controls in place for physical security, electronic security, and business continuity at the organizations assessed. We did not test these controls by attempting to gain unauthorized entry or access to facilities or information systems, or directly observe testing of business continuity capabilities.

We performed our work from September 2003 through August 2004 in accordance with generally accepted government auditing standards.

Role of the Department of Homeland Security

The Department of Homeland Security (DHS), created to help coordinate the efforts of organizations and institutions involved in protecting the nation against terrorist attacks, has essentially delegated to Treasury this coordinating role within the banking and finance sector. In 2002, the Homeland Security Act created DHS, which was given responsibility for developing a national plan to protect the nation's critical infrastructure. Homeland Security Presidential Directive 7 (HSPD-7), issued in December 2003, further stated that the Secretary of DHS, would be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure of the United States.¹ HSPD-7 also stated that it is U.S. policy to enhance the protection of these critical infrastructures against terrorist attacks that could, among other things, damage the private sector's capability to ensure the orderly functioning of the economy.

To fulfill these objectives, HSPD-7 directs the Secretary of DHS to work closely with other federal departments and agencies, and designates specific agencies to coordinate efforts within certain sectors. Within the banking and finance sector, Treasury was given responsibility for collaborating with all relevant federal, state, and local officials, as well as the private sector. To fulfill this responsibility, Treasury coordinates with other federal financial regulators through the Financial and Banking Information Infrastructure Committee (FBIIC), whose members include representatives of the various regulators of banks, broker-dealers, futures commission merchants, and housing government sponsored enterprises, as well as other related organizations.² Treasury coordinates its collaboration with the private sector through the Financial Services Sector Coordinating Council (FSSCC), whose members include representatives from exchanges, clearing organizations, and banking and securities trade associations.

¹*Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection* (Washington, D.C.: Dec. 17, 2003).

²These organizations include the Commodity Futures Trading Commission, the Conference of State Bank Supervisors, Treasury, the Farm Credit Administration, the Federal Deposit Insurance Corporation, the Federal Housing Finance Board, the Federal Reserve Bank of New York, the Federal Reserve, the Homeland Security Council, the National Association of Insurance Commissioners, the National Credit Union Administration, the North American Securities Administrators Association, the Office of the Comptroller of the Currency, the Office of Federal Housing Enterprise Oversight, the Office of Thrift Supervision, the Securities and Exchange Commission, and the Securities Investor Protection Corporation.

According to Treasury officials, they coordinate with DHS in several ways. For example, a FBIIC member attends weekly meetings of DHS's Directorate of Information Analysis and Infrastructure Protection (IAIP), which identifies and assesses threats and issuing timely warnings on those threats. According to Treasury, the FBIIC member at those meetings provides input on the needs of the financial sector as well as the relevancy for that sector of any identified threats. In addition, Treasury has worked with DHS to plan disaster recovery exercises, such as the TOPOFF exercises, which simulate physical attacks. Treasury is also working with DHS to continue developing "Chicago First," an emergency preparedness program designed to coordinate activities among financial sector participants and federal, state, and local government officials. Treasury is promoting this program as a model for other cities to implement. Finally, the Secretary of the Treasury, along with the Director of the Office of Homeland Security is a member of the Homeland Security Council, which ensures the coordination of homeland security activities among executive departments and agencies. Representatives of the Homeland Security Council, in turn, are members of FBIIC.

According to FSSCC officials, they are interacting with DHS in at least two ways. First, DHS has asked FSSCC to prepare an updated version of the banking and finance sector's portion of the national strategy for critical infrastructure assurance, the first version of which was completed in May 2002. FSSCC expected to complete the updated version in June 2004. Second, FSSCC representatives have taken part in quarterly meetings between DHS and other sector coordinators. According to FSSCC officials, this group has produced a matrix outlining the responsibilities of the different sectors.

Comments from the Federal Reserve



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

STEPHEN F. MALPHRUS
STAFF DIRECTOR FOR MANAGEMENT

September 10, 2004

Ms. Davi M. D'Agostino, Director
Financial Markets and Community Investment
U.S. Government Accountability 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 *Financial Market Preparedness: Improvements Made, But More Action Needed to Prepare for Wide-Scale Disasters*. Addressing the risks posed by the events of September 11 continues to be a priority for the Federal Reserve. As the draft report notes, we are also continuing efforts to improve the resilience of the financial system.

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 "Stephen F. 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



THE CHAIRMAN

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

September 16, 2004

The Honorable David M. Walker
Comptroller General of the
United States
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Walker:

This letter responds to the request to review and comment on the draft report entitled FINANCIAL MARKET PREPAREDNESS: Improvements Made, But More Action Needed to Prepare for Wide-Scale Disasters (GAO-04-984).

I appreciate the opportunity to respond to your report and I 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, core clearing organizations, and the major market participants to strengthen their resiliency. I am pleased that the GAO finds the markets to have made progress in telecommunications resiliency, physical controls, and business continuity planning.

The draft report makes four recommendations. The GAO's first recommendation is that the SEC should fully analyze the readiness of the securities markets to recover from major disruptions and work with the industry and other federal agencies, as appropriate, to determine reasonable actions that would increase the likelihood that trading in the markets would resume when appropriate. Accordingly, I have directed the staff to begin an assessment of key broker-dealers' trading staff arrangements and their ability to be prepared to resume their trading operations following a disaster. This assessment should be completed during the first half of 2005.

The GAO's second recommendation is for the SEC to establish a definite time frame for the submission of a rule requiring exchanges and clearing organizations to engage in activities consistent with the operational practices and other tenets of the ARP program. To that end, I understand that the Division of Market Regulation ("Division") is developing an automation rule proposal and that the proposal will be ready for Commission consideration during the first half of 2005.

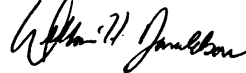
The GAO's third recommendation is for the SEC to assess the adequacy of ARP staffing in terms of positions and technical skill levels, including information security

The Honorable David M. Walker
Page 2

expertise, given its mission and workload. In this regard, a staffing assessment is currently underway in terms of positions. I understand the Division is also in the process of performing an assessment of technical skill levels needed, including information security expertise. Should this assessment find the need for greater information security expertise, or other technical skill levels, we would address that through a combination of continuing professional education of current staff, hiring new staff with the needed expertise, and hiring contractors with the appropriate level of expertise. Further, as technical skill levels and focus are constantly changing, we will continue to monitor where our resources are most needed. To help improve our inspections, we are always looking for new skills, standards, and guidelines to use in the information security and other IT areas.

Finally, the GAO recommends that the Commission continue to assess the organizational alignment of the ARP program within the SEC. In 2003, the Commission performed an extensive assessment of the functions, duties, and responsibilities of the entire Commission, including the ARP program. Based on that assessment, we created the Office of Market Continuity in the Division of Market Regulation into which the ARP functions were moved. This realignment has helped focus ARP issues, such as continuity of operations planning, business continuity planning, and market watch, in one office. As part of the Commission's routine strategic planning effort, we will continue to assess the organizational alignment of the ARP program.

Sincerely,



William H. Donaldson
Chairman

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, Gerald Barnes, Lon Chin, West Coile, Kevin E. Conway, Kirk Daubenspeck, Ramnik Dhaliwal, Patrick Dugan, Edward Glagola, Harold Lewis, Thomas Payne, Barbara Roesmann, Eugene Stevens, Patrick Ward, Christopher Warweg, and Anita Zagraniczny made key contributions to this report.

Related GAO Products

Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors. [GAO-04-699T](#). Washington, D.C.: April 21, 2004.

Securities and Exchange Commission: Preliminary Observations on SEC's Spending and Strategic Planning. [GAO-03-969T](#). Washington, D.C.: July 23, 2003.

Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants. [GAO-03-251](#). Washington, D.C.: February 12, 2003.

Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants. [GAO-03-414](#). Washington, D.C.: February 12, 2003.¹

Critical Infrastructure Protection: Effort of the Financial Services Sector to Address Cyber Threats. [GAO-03-173](#). Washington, D.C.: January 30, 2003.

SEC Operations: Increased Workload Creates Challenges. [GAO-02-302](#). Washington, D.C.: March 5, 2002.

A Model of Strategic Human Capital Management. [GAO-02-373SP](#). Washington, D.C.: March 15, 2002.

Information Systems: Opportunities Exist to Strengthen SEC's Oversight of Capacity and Security. [GAO-01-863](#). Washington, D.C.: July 25, 2001.

Homeland Security: Efforts to Improve Information Sharing Need To Be Strengthened. [GAO-03-760](#). Washington, D.C.: June 29, 2001.

Human Capital: A Self-Assessment Checklist for Agency Leaders, Version 1. [GAO/OCG-00-14G](#). Washington, D.C.: September 2000.

Federal Information System Controls Audit Manual, Volume I: Financial Statement Audits. [GAO/AIMD-12.19.6](#). Washington, D.C.: January 1999.

Executive Guide on Information Security Management: Learning from Leading Organizations. [GAO/AIMD-98-68](#). Washington, D.C.: May 1, 1998.

¹This report contains information identical to [GAO-03-251](#).

GAO's Mission

The Government Accountability Office, the audit, evaluation and 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 GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

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. Government Accountability 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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

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

**United States
Government Accountability Office
Washington, D.C. 20548-0001**

**Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00**

**Official Business
Penalty for Private Use \$300**

Address Service Requested

