United States Government Accountability Office

GAO

Report to Congressional Requesters

March 2007

FINANCIAL MARKET PREPAREDNESS

Significant Progress Has Been Made, but Pandemic Planning and Other Challenges Remain

GAO-07-399

March 2007

FINANCIAL MARKET PREPAREDNESS

Significant Progress Has Been Made, but Pandemic Planning and Other Challenges Remain

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-399, a report to congressional requesters

Why GAO Did This Study

This is GAO's third report since the September 11 terrorist attacks that assesses progress that market participants and regulators have made to ensure the security and resiliency of our securities markets. This report examined (1) actions taken to improve the markets' capabilities to prevent and recover from attacks; (2) actions taken to improve disaster response and increase telecommunications resiliency; and (3) financial regulators' efforts to ensure market resiliency. GAO inspected physical and electronic security measures and business continuity capabilities using regulatory, government, and industry-established criteria and discussed improvement efforts with broker dealers, banks, regulators, telecommunications carriers, and trade associations.

What GAO Recommends

To improve the readiness of the securities markets to withstand potential disease pandemics, securities and banking regulators should consider taking additional actions, including providing formal expectations that market participants' plans address even severe pandemic outbreaks and setting a date by which such plans should be completed. Banking and securities regulators indicated they believe organizations are adequately addressing this risk, but will consider taking the recommended actions if progress lags. GAO believes that giving greater consideration now would better assure market readiness.

www.gao.gov/cgi-bin/getrpt?GAO-07-399.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Yvonne D. Jones at (202) 512-8678 or jonesy@gao.gov.

What GAO Found

The critical securities markets organizations GAO reviewed have acted to significantly reduce the likelihood of physical disasters disrupting the functioning of U.S. securities markets. As of January 2007, the seven critical exchanges, markets, clearing organizations, and payment processors GAO reviewed have the capability of performing their critical functions at sites that are geographically dispersed from their primary sites. These organizations were also preparing plans to reduce the likelihood that a disease pandemic will disrupt their critical operations, although not all had fully completed such efforts. They also improved their physical and information security measures, including by taking actions that GAO identified during this review. Although key securities trading staff remain concentrated in single locations, the broker-dealers and clearing services banks that account for significant trading volumes and that GAO reviewed have increased the distances between their sites for primary and backup operations for clearance and settlement activities and established dispersed backup trading locations.

Various private and public sector groups continued to enhance the preparedness of the financial sector, although resolving vulnerabilities in the telecommunications infrastructure remains a challenge. Securities industry organizations have continued to conduct annual industrywide tests of financial market participants' backup site operating capabilities, and key trading and clearing organizations are increasingly using communications networks that are less vulnerable to disruption to transmit information. After attempts to assist individual financial market participants to determine whether their own telecommunications lines were routed through single paths or switches proved difficult, regulators are assisting efforts to develop automated systems for identifying circuit paths. In response to concerns over whether the telecommunications infrastructure can absorb the increased demand likely to result from large numbers of organizations and individuals seeking to telecommute during a pandemic, financial regulators and market participants are assisting government efforts to model such events and develop potential solutions.

To improve market resiliency, financial regulators established goals for prompt recovery of critical clearing activities after disasters and have been conducting examinations to ensure market participants' compliance. Securities regulators also set goals and are examining securities markets' readiness to resume trading and plan to do more focused reviews of individual broker-dealer capabilities. SEC also has improved its program for overseeing operations issues at market and clearing organizations, including increasing its staffing levels and expertise. Securities and banking regulators have been actively addressing pandemic issues, but could better ensure that market participants prepare complete plans and have sufficient time to train employees and test these plans, by providing formal expectations that plans address even severe outbreaks and set dates for completing such plans.

Contents

Abbreviations

ARP	Automation Review Policy
ATIS	Alliance for Telecommunications Industry Solutions
CDC	Centers for Disease Control and Prevention
DHS	Department of Homeland Security
FBIIC	Financial and Banking Information Infrastructure Committee
FS/ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security
NCS	National Communications System
NSTAC	National Security Telecommunications Advisory Committee
NYSE	New York Stock Exchange
OCC	Office of the Comptroller of the Currency
SEC	Securities and Exchange Commission
SMART	Securely Managed and Reliable Technology
SFTI	Secure Financial Transaction Infrastructure
SIA	Securities Industry Association
SRO	Self-regulatory organization
TSP	Telecommunications Service Priority
WHO	World Health Organization

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 29, 2007

Congressional Requesters:

The massive destruction caused by the September 11, 2001, terrorist attacks on the World Trade Center showed how the financial markets can be significantly affected by such events. In several prior reports since the attacks, we found that financial market participants—including the exchanges, clearing organizations, and broker-dealers and banks that conduct trades and process payments—and regulators had taken many actions to reduce the risk that such disasters would disrupt the markets' operations in the future.[1] However, we also reported that some of the organizations that execute trades or perform clearance and settlement processing essential to the functioning of the U.S. securities markets lacked backup operating sites sufficiently distant from primary operating locations, and thus were at a greater risk of disruption from wide-scale events such as terrorist attacks or natural disasters that physically damage facilities and infrastructure over a wide area. In addition, we reported that although the broker-dealers that account for significant trading volumes and the clearing banks that process payments associated with trading also increased their ability to resume operations after such events, some still were vulnerable to disruption by such disasters.

As a result, our September 2004 report included recommendations to the Securities and Exchange Commission (SEC) to assess whether the improvements various broker-dealers implemented would be sufficient to allow trading to resume after a disaster. In addition, we recommended that SEC make various improvements to the program and staff that it uses to oversee market security and business continuity issues. To assess whether market participants and regulators have continued to ensure the security

[1]See 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). These reports provide identical information, so, for simplicity, we will refer to them throughout this report as our 2003 report. Also see *Financial Market Preparedness: Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters*, GAO-04-984 (Washington, D.C.: Sept. 27, 2004) and see *Financial Market Organizations Have Taken Steps to Protect against Electronic Attacks, but Could Take Additional Actions*, GAO-05-679R (Washington, D.C.: June 29, 2005).

and resiliency of our securities markets, you asked that we conduct a review to document the progress these organizations have made since our last report. Specifically, we assessed (1) actions critical securities market organizations and key market participants have taken to improve their business continuity capabilities for recovering from physical disasters, electronic attacks, and pandemics and the measures they use to reduce their vulnerabilities to such events; (2) actions taken by financial market participants, telecommunications industry organizations, and others to improve the ability of participants to respond to future disasters and increase the resiliency of the telecommunications on which the markets depend; and (3) financial regulators' efforts to ensure the resiliency of the financial markets, including SEC's progress in improving its securities market organization oversight program.

In performing this work, we visited seven organizations—which included exchanges, clearing organizations, and payment system processors—that we categorized as critical because the products or services they offered or 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 regulator-established criteria or criteria generally accepted by government or industry. For our reviews, we reviewed documentation and descriptions that market participants and regulators provided and reviews that other organizations—such as external consultants or other government agencies—had conducted. 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; we also did not directly observe testing of business continuity capabilities. In addition to the critical organizations, we also discussed the business continuity capabilities and improvements of six large broker-dealers and banks, which collectively represented a significant portion of trading and clearing volume for U.S. securities markets. In addition, we reviewed documents from financial market regulators, industry associations, a major telecommunications carrier, the Department of the Treasury, and the Department of Homeland Security, and interviewed their staffs about actions they have taken to improve the resiliency of the financial markets and telecommunications service. To assess regulators' oversight efforts, we reviewed relevant regulatory guidance and examinations done by banking and securities regulators of financial market organizations and key participants. We performed our

work from April 2006 through February 2007 in accordance with generally accepted government auditing standards. For more information on the scope and methodology of our review, please see appendix I. For security reasons, we did not include the names of the organizations we reviewed or their functions and locations in this report.

Results in Brief

Since our last report, the organizations whose operations are critical to the securities markets as well as key broker-dealers and banks that participate in these markets have worked to significantly reduce the likelihood that wide-scale physical disasters would disrupt the functioning of U.S. securities markets, and have been actively planning to similarly withstand an influenza pandemic although few had fully completed their plans. As of now, all seven critical exchanges, clearing organizations, and payment processors that we reviewed reported having acquired the capability to conduct their operations from alternate sites that include adequate systems and staff to perform their critical functions and are geographically dispersed from their primary sites. These organizations also are working on planning and preparation efforts to reduce the likelihood that a worldwide influenza epidemic—known as a pandemic—would disrupt their critical operations, although only one of the seven had completed a formal plan.[2] To limit the potential for physical attacks to disrupt their operations, all the critical organizations have continued to enhance their physical security measures and those with remaining vulnerabilities have mitigated these with business continuity capabilities. These organizations also have continued to improve their information security measures by making progress in areas we previously had identified and agreed to address some additional areas we identified during this review. Similarly, key broker-dealers and clearing banks that we reviewed also have increased the distance between the sites for primary and backup operations they use to conduct securities clearance and settlement activities. Although keeping trading staff concentrated in single locations increases the risk that a wide-scale disaster or a pandemic could prevent trading activities from being resumed promptly, the key broker-dealers we reviewed had taken other steps to reduce their vulnerability to physical disasters by establishing backup trading locations away from their primary sites. They also were taking additional actions, including training staff they

[2]An influenza pandemic is characterized by the emergence of a novel influenza virus to which much or all of the population is susceptible, is readily transmitted person to person, and causes outbreaks in multiple countries.

have in other locations, such as overseas, to conduct trading in U.S. securities if necessary.

Securities market participants, industry organizations, government agencies, and telecommunications carriers have continued to enhance the readiness and resiliency of the financial sector, although resolving some vulnerabilities of the telecommunications infrastructure remains challenging. To provide assurance that securities market participants can perform critical activities in the event of a disaster, securities industry organizations have continued to oversee annual industrywide tests that assess market participants' ability to connect to and process transactions from all participants' backup sites. The Department of Homeland Security also has been conducting physical security assessments at various financial market organizations and included financial market participants and regulators in several disaster simulations. The telecommunications resiliency of critical financial market organizations also has grown as customers increasingly connect to them at multiple points on external communications networks designed to withstand damage. Although financial regulators and telecommunications organizations have assessed the viability of mapping the physical paths of financial market organizations' telecommunications circuits as a means of ensuring more secure redundant routing, such efforts have proven to be time-consuming and expensive. Concerns also have been raised about whether the telecommunications infrastructure is adequate to handle the increased traffic likely to result from large numbers of organizations and individuals attempting to telecommute during a pandemic. However, financial market participants and government agencies are involved in initiatives to develop potential solutions to these challenges.

Financial regulators have worked to improve the readiness and resiliency of the securities markets by issuing guidance and conducting examinations focusing on clearing activities and trading markets. Working jointly, banking and securities regulators issued guidance that established expectations for prompt recovery of critical clearance and settlement activities and conducted examinations of the key clearing organizations, the banks, and broker-dealers with significant clearing and trading volumes to ensure that these organizations have been complying with this guidance. By finding that most organizations were already or soon expected to be fully compliant, regulators have taken a significant step in ensuring that a wide-scale disaster would not result in a cascade of payment failures that could result in a systemic crisis. SEC and the banking regulators have issued general statements that advise the financial entities they oversee to develop business continuity plans for pandemics

and indicated that they are reviewing the pandemic-planning efforts of market organizations, broker-dealers, and clearing organizations as part of their ongoing supervisory exams and related activities. Although regulators and market participants have taken many actions to prepare the markets to continue operations during a pandemic, further action could improve market readiness. Although regulatory staff told us that they are discussing their expectations regarding pandemic plans in meetings and public forums and during ongoing supervisory activities, the formal statements that these regulatory agencies have issued do not specifically direct organizations to prepare plans likely to be effective during even severe outbreaks, nor have they established a date by which these plans should be completed. If organizations fail to produce fully robust plans before an outbreak—which could begin at any time—they may have insufficient time and resources to adequately prepare their staffs and customers for changes in how the organizations will operate during a pandemic. In response to our previous report's recommendation, SEC staff reported that they explored the steps that broker-dealers have taken in light of various physical disaster scenarios and also have developed additional examination procedures that they expect to use in future examinations to better assess broker-dealer trading readiness. Since our last review, SEC also has improved the Automation Review Policy (ARP) program that it uses to oversee clearing and market organizations. SEC increased the size and expertise levels of its staff and contracted with external consulting organizations to perform reviews of the entities ARP oversees. Also, as we recommended, SEC drafted a rule that would require adherence to ARP program tenets; the rule has been undergoing internal reviews and is expected to be submitted to the SEC Commissioners for final approval in spring 2007.

While considerable progress has been made, continued attention by regulators is warranted. We are encouraged by their ongoing efforts to address the remaining challenges, including improving telecommunications resiliency and ensuring broker-dealer trading readiness. To further improve the financial markets ability to withstand pandemic disease, this report recommends that the banking and securities regulators consider taking various actions—including providing specific expectations to financial market organizations and market participants that business continuity plans for pandemics should include measures likely to be effective even during severe outbreaks and setting a date by which formal plans for disease outbreaks should be completed. Such guidance also should encourage organizations to develop plans flexible enough to effectively address a range of possible effects and responses that could result from such events. In a letter commenting on a draft of

this report, officials from the Federal Reserve, OCC, and SEC acknowledged that they shared our views on the importance of ensuring that the financial markets enhance their resiliency and appreciated our recognition that significant progress has been made. Regarding our recommendation, the officials noted that the critical organizations and key market participants are planning for a pandemic, including a severe outbreak, and identifying measures to reduce their vulnerabilities to such events. The regulators also noted that they are reviewing these organizations' progress and they believed that these organizations' contingency plans generally address the four elements recommended in our report. The regulatory officials stated that they will follow up to ensure any weaknesses in the ongoing pandemic-planning process are appropriately addressed by the organizations, and if they find that organizations' efforts are lagging, they will consider taking additional actions, including those that we have suggested. We are encouraged that the regulators plan to actively monitor the progress that critical organizations and key market participants are making to plan and prepare for a pandemic. However, recent reviews of at least one critical organization's pandemic plan and contacts with representatives of the six key market participants indicated that some organizations may not yet be fully prepared or potentially may fail to consider all potential pandemic scenarios, particularly if the difficulty in mitigating certain scenarios discourages or delays firms' willingness to fully prepare. As a result, we continue to believe that having regulators give greater consideration to providing specific instructions to market participants and setting a date for pandemic continuity plan completion would increase the likelihood that organizations fully prepare and have adequate time to test and adjust any planned responses in advance of the outbreak of an actual pandemic.

Background

Various organizations must be able to operate for the U.S. securities markets to function. Individual investors and institutions such as mutual funds send their orders to buy and sell stocks and options to broker-dealers, which route them to be executed at one of the many exchanges or electronic trading venues in the United States. After a securities trade is executed, the process known as clearance and settlement occurs that ensures the accuracy of the trade, transfers ownership of the securities from the seller to the buyer, and exchanges the necessary payment between these two parties. Separate organizations perform this process for stocks and for options, while a single depository maintains records of ownership for the bulk of the securities traded in the United States. Banks 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. The payments that are exchanged between the banks of clearing organizations, broker-dealers, and their customers are processed by systems operated by the Federal Reserve or other private payment system processors. Virtually all of the information processed is transferred between parties through telecommunications systems; as a result, the securities markets depend heavily on the telecommunications industry's supporting 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 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 might be limited to a reduced liquidity or less 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. 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 (SRO) for ensuring that their participants comply with the securities laws and these organizations' own rules. To oversee the operational risks at the securities exchanges and clearing organizations, SEC published its Automation Review Policy in 1989, which advised SROs prospectively of SEC's expectations on how these organizations should address information dissemination and

physical security and business continuity challenges.[3] ARP staff conduct reviews of how these organizations are addressing SEC's expectations in these areas. 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.

To ensure that the functioning of the financial markets is protected, the financial sector is one of several key infrastructures that the United States has designated as critical to our nation. To protect these infrastructures, the Homeland Security Act of 2002 created the Department of Homeland Security (DHS) and gave it wide-ranging responsibilities for leading and coordinating the overall protection effort for the nation's critical infrastructure.[4] Homeland Security Presidential Directive 7 further defines these responsibilities for DHS and those federal agencies given responsibility for particular industry sectors such as telecommunications or banking and finance, known as sector-specific agencies. The Department of the Treasury (Treasury) is the federal agency responsible for infrastructure protection activities in the banking and finance sector, which includes coordinating and collaborating with relevant federal agencies, state and local governments, and the private sector.

The threats for which organizations in the financial and other critical sectors must be prepared vary. As the events of September 11 illustrated, terrorist activity can pose a significant threat to U.S. entities. Events such as attempts to bomb key facilities can significantly impair the operations of an affected organization and events involving nuclear, radiological, or chemical hazards could cause substantial damage to key facilities or necessary infrastructure over a wide area or render such facilities and infrastructure inaccessible for extended periods. Similarly, major natural disasters such as hurricanes, tornados, or earthquakes also can result in wide-scale damage or make areas inaccessible just about anywhere in the United States. In addition to events that cause physical damage, financial

[3]Automated Systems of Self-Regulatory Organizations, Exchange Act Release No. 27445 (Nov. 16, 1989), republished in 54 Fed. Reg. 48703 (1989) (Policy Statement). General statements of policy are statements issued by an agency to advise the public prospectively of the manner in which the agency proposes to exercise a discretionary power.

[4]Pub. L. No. 107-296, 116 Stat. 2135 (2002).

market organizations remain a prime target for individuals or organizations seeking to use cyber attacks to obtain unauthorized access or prevent legitimate users from accessing the key networks and systems upon which the financial markets depend. Moreover, concern has grown about the threat of an influenza pandemic and the impact it could have on the operations of entities in the United States, including those in the financial markets. With individuals in other countries having already have fallen ill and died as a result of the H5N1 strain of avian flu, the U.S. government is urging all businesses to prepare for a pandemic. The pandemic threat is different than those previously envisioned because it could affect large numbers of people simultaneously, with waves of illness occurring for weeks at a time over the course of several months.

Financial Market Organizations Have Significantly Improved Their Ability to Withstand Physical Disasters, Although Pandemic Planning Remains Challenging

Since our last report, all seven organizations whose operations we considered critical to the overall functioning of U.S. securities markets have in place business continuity capabilities that reduce their vulnerability to disruption by a wide-scale disaster. These capabilities include having backup operating sites that have staff capable of performing the organizations' critical tasks and that are geographically distant from their primary operating locations. All seven critical organizations have taken steps to reduce the likelihood that power and telecommunications outages will affect their operations and all have tested their business continuity capabilities by running simulations or performing live processing of their primary activities from backup locations. All seven critical organizations are developing business continuity plans to address the risk of infectious pandemics, although at the time we reviewed these organizations only one had fully developed a plan that incorporates the various elements needed to address such an occurrence. Each of the seven organizations also has continued to enhance the measures it uses to prevent physical attacks from disrupting its operations, with those that still had vulnerabilities using their business continuity capabilities to mitigate those weaknesses. Each organization continued to improve the information security measures intended to mitigate the risk of electronic attacks, including taking or considering additional actions we identified that could further improve their information security. Representing many of the most active market participants, the large broker-dealers and banks that we contacted also have continued to improve their disaster-recovery capabilities. Although by maintaining their trading staff in single locations increases the risk that they will be unable to resume activities promptly after a wide-scale disaster, the major broker-dealers we reviewed have implemented various

measures to mitigate such risks, including cross-training staff and establishing dispersed backup trading locations.

Critical Financial Market Organizations Have Developed Business Continuity Capabilities to Help Address the Risk of Wide-Scale Disasters

Since our 2004 report, all the critical organizations have established business continuity capabilities that reduce the likelihood that a wide-scale physical disaster would disrupt their key operations. When we last reported, four of the seven organizations had established backup sites capable of performing the key activities they needed to be operational and located them at considerable distances from their primary sites to reduce the likelihood that a disaster, even a wide-scale event, would render both locations unusable. However, at that time, we also reported that three of the critical organizations lacked business continuity capabilities that likely would have allowed them to resume operations shortly after such disasters. For example, one of these organizations had a backup site that it could use to conduct its key activities, but this site was within a few miles of its primary location and therefore also could have been rendered unusable in a wide-scale disaster.

As of September 2006, all seven critical organizations now have geographically distant backup sites or other means of conducting their key operations. For example, one of the organizations previously lacking a geographically dispersed site has completed a new data center that is more than 1000 miles from its primary operating locations and that now is capable of conducting all the key processing that the organization would need to be operational. Because the distance between sites is too great to allow both the primary and the backup site to process identical data simultaneously, the organization has implemented a proprietary hardware based data replication technology that ensures that copies of all production data and processing results from the primary sites are stored and then transmitted to the remote site.[5] Since installing this technology, the organization's staff indicated that it has significantly reduced the time required to have the remote site take over operations to less than 2 hours with less than a minute of data loss if a disaster were to affect both primary processing sites. Rather than establishing a geographically distant

[5]As the result of transmission speed limitations, the distance between two operating sites receiving identical data and processing transactions simultaneously—called synchronous sites—generally is limited to about 50 or 60 miles. To ensure that back up sites outside of this range have the complete data and results of the primary site, organizations generally must use technology that copies the primary site's data as they are being processed and then transmits the copied data to any backup locations.

site that exactly duplicates its primary site, another of these three organizations instead acquired the capability to conduct its critical trading activities through an electronic system whose processing location is located more than 700 miles from the organization's current operating site. Finally, to better ensure that it would be able to operate in the aftermath of a wide-scale disaster, the last of these three organizations installed hardware capable of performing its critical processing operations at a site that is more than 200 miles from its current primary operating location.

In addition to these three organizations, the other four have also improved their business continuity capabilities to further reduce their vulnerability to such events. For example, one organization that when we last reported had established a backup data center more than 700 miles from its headquarters and primary operating location changed how it operates so that it now conducts its live critical business processing from the geographically distant site and uses its former primary processing site as its backup location. According to the staff of this organization, they transferred the operations to the more distant site because it is located in an area they deemed at lower risk than its current headquarters and former processing location, which is located in a downtown urban area that they believe is more likely to be at risk for terrorist activities than the new primary processing location. Although the organization likely may have reduced its risk of disruption from terrorist activities, its new primary location may be at greater risk of damage from natural disasters, such as hurricanes or tornados, than its headquarters location. When we last reported, another of the critical organizations had three locations at which it could conduct its critical processing operations; a primary operating site, a secondary site that could quickly take over processing if a disaster damaged the primary site, and a tertiary site that could become operational within 24 hours if the backup site were not available. Since then, this organization lowered its vulnerability to disruption by changing the configuration of its data centers to provide greater distance between its primary and secondary sites, increasing the distance between these sites by hundreds of miles. In addition, two organizations have increased their recovery capabilities by establishing sites hundreds of miles from the primary site that are capable of monitoring and operating critical networks at the primary location. These remote command centers give the organizations the ability to maintain or resume operations if their primary site became inaccessible, but was not destroyed.

By establishing these dispersed operating capabilities, all the organizations have addressed another potential weakness—the concentration of staff in one location or a geographic area—that previously increased their

vulnerability to a wide-scale disaster. When we last reported in 2004, several of the critical organizations faced greater risk that their operations could be disrupted by disasters because the staff they needed to perform their critical business operations were located in just one location or in multiple locations near each other. However, now all seven organizations have taken steps to ensure that they will have staff capable of performing their critical activities in the event of a wide-scale disaster, either by establishing backup operating locations or making other arrangements to have sufficient staff to conduct the organizations' critical operations. These operations include backup data-processing centers and alternative site business operating centers that have staff that perform critical non-data-processing activities, such as assisting customers or performing activities requiring manual processing.

Critical Organizations also Have Improved Their Telecommunications and Power Resiliency and Tested Their Business Continuity Capabilities

The seven critical market organizations also have reduced the likelihood that their operations would be disrupted by disasters that affect their power or telecommunications services. For example, all organizations installed generators capable of supplying their operations sites with power if they lose power from their local utility. These organizations generally had fuel supplies on hand that would be sufficient to run these generators from 3 to 7 days. During the August 2003 power failure that affected the Northeast, all seven critical organizations successfully provided service to their customers and members without interruption.

Similarly, the organizations also all have taken steps to reduce the likelihood that they would lose their telecommunications service. For example, all the organizations had registered the circuits that carry their important telecommunications traffic with the National Communications System's Telecommunications Service Priority (TSP) program, which would provide increased priority for restoration of these key circuits in the event of a disruption. Several of the organizations also now increasingly receive information from their members through more resilient telecommunications networks. For example, the Secure Financial Transaction Infrastructure (SFTI) was created to provide a more reliable and "survivable" private communications network that links exchanges, clearing organizations, and other financial market participants. To ensure resiliency and eliminate single points of failure, SFTI employs redundant equipment throughout, and carries data traffic over redundant fiber-optic rings that have geographically and physically diverse routes. To improve the resilience of the communications for clearing securities transactions, the Securely Managed and Reliable Technology (SMART) network has been created that allows market participants to exchange information with clearing organizations over private high-bandwidth networks that

automatically route traffic over alternate paths in the event that any part of the network is damaged. In addition, one of the critical organizations we reviewed formerly received data from its broker-dealer customers through direct connections to its data centers—often from just a single customer's location. However, this organization now has a network configuration in which the customers connect at multiple points to a new redundant fiber-optic ring network, reducing the likelihood that customers would be unable to communicate with the organization.

Moreover, the seven critical organizations have tested their business continuity capabilities and plans—although some more fully assessed the ability of their backup arrangements than others. Routinely using or testing recovery and resumption arrangements ensures that backup arrangements can perform critical operations and that all customers or others that must connect to an organization are able to do so. Some of the critical organizations have conducted very robust testing of their ability to operate from other locations outside their primary location. For example, at least two of the critical organizations operated data centers that receive all the data needed to process their operations and had run live processing for actual business days from their non-primary locations. In contrast, another organization regularly tested the operational condition and connectivity of its equipment at its back up site and ran exercises with small numbers of staff at this site to simulate its critical activities, but had never attempted to conduct an actual business day from this backup location. One organization had used the systems it would need to operate if its primary location were damaged for some live processing but had not yet fully tested whether these systems had adequate capacity to process the organization's full operating volume of data.

Critical Organizations also Have Begun to Address Risk of Pandemics

In recognition of the increased concerns of a pandemic influenza outbreak, the seven critical organizations also were in the process of developing business continuity plans to address the potential impacts of a pandemic on their operations, although only one has completed a formal plan. To determine elements that could be considered as part of business continuity planning for a pandemic, we identified various documents issued by private sector organizations, government bodies, and financial

regulators.[6] These included a paper issued by the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), which includes representatives of various financial market trade associations, market organizations, and others. The FSSCC pandemic paper outlined numerous issues that organizations should consider, as well as one issued by a risk and insurance services firm that included actions to consider taking before, at onset, and throughout the event. In addition, we reviewed issuances by U.S. banking regulators, as well as those from other U.S. and international organizations.

By analyzing these documents, we identified four elements that we used to evaluate the seven critical financial market organizations' pandemic planning efforts, including:

- A preventive program to reduce the likelihood that an organization's operations will be affected, including monitoring of potential outbreaks, educating employees on the disease and how to minimize its transmission, and providing disinfectant soaps and hand sanitizers in the work place.

- A formal plan that includes escalating responses to particular stages of an outbreak, such as first cases of humans contracting the disease overseas, first cases within the United States, and first cases within the organization itself.[7]

- Facilities, systems, or procedures that provide the organization the capability to continue its critical operations in the event that large

[6]The guidance we considered in evaluating organizations' pandemic planning disease scenarios included: (1) Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, *Statement on Preparations for Avian Flu*, (Jan. 24, 2006); (2) the Federal Reserve System Board of Governors, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, *Interagency Advisory on Influenza Pandemic Preparedness*, (Washington, D.C.: Mar. 15, 2006); (3) T. Walsh, "Avian Flu: Preparing for a Pandemic," *Marsh Risk Alert 5, no. 1* (Jan. 2006); (4) Department of Health and Human Services, the Centers for Disease Control and Prevention, *Business Pandemic Influenza Checklist*, http://www.pandemicflu.gov/plan/pdf/businesschecklist.pdf, (accessed April 24, 2006); (5) Department of Homeland Security, *Pandemic Influenza Preparedness, Response, and Recovery Guide to Critical Infrastructure and Key Resources*, (Washington, D.C.: Sept. 19, 2006); (6) International Monetary Fund, *The Global Economic and Financial Impact of an Avian Flu Pandemic and the Role of the IMF*, Washington, D.C.: (Feb. 28, 2006).

[7]For example, pandemic plans could be pegged to the stages or phases of an outbreak that are designated by the World Health Organization, the Centers for Disease Control, or the Department of Health and Human Services.

numbers—as many as 40 percent by some estimates—of an organization's staff will be unavailable for prolonged periods. Such procedures could include social distancing to minimize staff contact, teleworking, or conducting operations from alternative sites.

- A testing program to better ensure that the practices and capabilities that an organization implements to address a pandemic will be effective and allow it to continue its critical operations.

The guidance that U.S. and international entities have issued also include other elements that organizations could take into account to produce an effective business continuity plan for a pandemic, including developing appropriate compensation and sick leave policies and establishing communication mechanisms, such as hotlines, to aid in providing information to employees and customers.

The seven critical organizations all were conducting activities to help them prepare business continuity plans to address pandemic risks. For example, one organization has begun to analyze which staff would be considered critical and how the organization could continue operations if as many as 70 percent of its total staff were not available—a higher percentage than some organizations are projecting could be affected. Staff at two of the organizations told us that they had begun training alternate staff to perform critical duties normally done by other staff. Staff at one of the organizations described conducting a "tabletop" exercise in which their staff discussed what actions they would take and what challenges they would face in a pandemic scenario. At the time we visited these organizations, only one of the seven organizations had a fully developed plan for addressing pandemic threats in place with detailed response plans for each business unit. Another of the organizations has a draft plan in place, although at this time it does not include information on how specific business functions will be maintained across varying absence levels. The other organizations, while not having formal plans completed, have gone through various planning efforts, such as verifying that staff can work from multiple locations and then expanding the number of communications channels available from remote locations as needed. Depending on how an influenza pandemic spreads, the impact on some of these organizations might somewhat be mitigated because of their existing dispersed business continuity capabilities. However, health organizations have cautioned that with global airline travel available, any disease outbreak could occur quickly and be widely spread within a short period of time, an occurrence that would reduce the protection that dispersed facilities provide.

Although Some Challenges Remain, Organizations also Have Acted to Reduce Physical Security and Information Security Vulnerabilities

The seven critical market organizations have continued to implement physical security measures to reduce the potential for physical attacks on their facilities. To assess the actions taken by the critical organizations since our last report, we discussed and inspected the security measures in place at these organizations. Based on these assessments, we found that organizations had continued to improve their physical security. For example, one organization has installed barriers that create a fixed holding area for vehicles undergoing security checks before allowing them to approach its facility. This same organization has reduced the likelihood that its facility will be damaged by bombs by installing thicker, more blast-resistant walls and glass. To further improve its security, another organization added a new armed security post to mitigate potential risks from nearby vehicular traffic and commercial sites and additional surveillance cameras capable of providing wider views of the area around its primary site.

But, some organizations continue to face challenges in limiting the potential for physical attacks on their facilities. For example, one organization is in the process of moving its primary and backup operations from its own secured facilities to sites that a contractor operates. Through inspection of one of these new facilities, we determined that it had various physical security measures in place, including a fenced perimeter and inspections of packages and visitors. However, this new site had less imposing barriers around it and was located closer to roads around the facility than the organization's previous primary operating site. Several of the other organizations also had continuing physical security vulnerabilities at their primary sites, such as being located in multitenant buildings or not having the ability to limit vehicular traffic around their facilities. However, the risk of any of these new or remaining physical security vulnerabilities at the seven organizations' primary sites largely has been mitigated by each having implemented geographically dispersed capabilities for conducting their critical activities.

The seven critical organizations also have continued to make progress in enhancing their information security. To assess the actions taken by the critical organizations since our last report, we reviewed documentation for any new systems, networks, and security measures at these organizations and discussed them with the organizations' staff. Based on these assessments, we determined that the seven organizations were continuing to implement sound information security practices, such as using firewalls or other controls to limit unauthorized access, expanding their use of systems to detect intrusions, conducting more extensive assessments of their systems' security vulnerabilities, and implementing the

improvements we identified in our previous reviews.[8] However, in some cases organizations have put in place new systems architectures that potentially introduce new vulnerabilities. As a result, we identified additional ways in which the organizations could improve their information security, measures that all the organizations either had begun implementing or were considering.

Broker-Dealers and Banks Have Reduced Risk of Disruption in Clearing Activities and Continue to Address Risks to Trading Activities

Since our 2004 report, the banks and broker-dealers that are key participants in the U.S. securities markets have made considerable progress in improving their resiliency, but certain wide-scale disasters could significantly disrupt their ability to conduct trading activities. We spoke with six firms, including four broker-dealers that conduct significant volumes of trading on U.S. securities markets, and two banks that are responsible for the clearance and settlement activities necessary to ensure that securities ownership and payments are appropriately transferred.[9] If firms such as the six described above were unable to conduct the processing needed to clear and settle securities transactions after a disaster, the resulting failures to pay for and deliver securities could lead other firms to be unable to make subsequent payments or deliveries, resulting in a potential systemic financial crisis. In addition, if sufficient numbers of broker-dealers were not able to resume trading activities when appropriate, the ability of U.S. trading markets to function could be impaired.

In response to expectations by financial regulators, since the 2001 attacks these broker-dealers and banks have improved the resiliency of their clearing and settling operations by increasing the geographic distance between the primary and backup sites that conduct such operations. For example, all six of the firms have established primary data centers in locations outside of New York City. In addition, one of these firms has established a new backup data center overseas. According to firm officials, all but one of these facilities are operational, with the last one to be completed by March 2007. Three of these firms have gone beyond regulators' expectations to establish a third data center that provides an additional level of backup for clearance and settlement activities. One firm

[8]See GAO-05-679R.

[9]One of the firms counted here as a bank also plays a significant market role as a broker-dealer. However, to avoid double-counting this firm, it is counted only once (as a bank) in this report.

has even established a fourth data center, and another has a fourth under construction. In addition, staff at all six firms told us that they routinely use or test their recovery and resumption arrangements to ensure that they can recover and resume their clearance and settlement activities within the time frames expected by the regulators.

Although firms have strengthened the resiliency of their clearing and settling operations, their trading activities remain vulnerable to disruption because all key trading staff are still concentrated in one geographic area. To conduct trading, broker-dealers generally operate trading floors where their traders receive orders from customers and enter these into electronic systems for execution at an exchange, electronic market, or other venue. The firms process the information the trading systems produce at data centers. Based on our discussions with these broker-dealers, these firms have established multiple data centers, including those outside the area. However, all these firms' key staff who trade U.S. stocks are located at trading floors in or near the New York City financial district.[10] Since the attacks on September 11, two of these firms moved their trading floors from lower Manhattan to midtown, which may reduce the risk of a trading disruption following a localized attack or other disaster in lower Manhattan. But, the stock traders still work in one relatively small geographic area and rely on some of the same infrastructure. For example, they share the same public transportation system. This concentration of traders poses a risk to trading activities because it could prevent firms from promptly resuming trading after a wide-scale physical disaster, a vulnerability that we initially noted in our 2004 report. (We discuss how SEC is addressing this risk later in this report.) Similarly, such staff are also at risk from a pandemic outbreak.

Nevertheless, the firms we reviewed have taken a variety of steps to mitigate the risks to their ability to trade. For example, all firms have implemented backup trading floors, which would allow them to conduct their trading activities at an alternate site if their primary trading floors were unusable or inaccessible. All of the firms have conducted some trading from their backup floors at least once, on occasions such as the 2004 Republican National Convention and the 2005 transit workers' strike (both of which events resulted in reduced accessibility to Manhattan). In addition, officials at one firm said that they have some ability to conduct trading in U.S. securities from an overseas location. According to SEC,

[10]Five of the six firms we reviewed conduct a significant volume of trading.

other firms also are exploring the possibility of conducting such trading from overseas. However, some of the firm officials with whom we spoke said that they were reluctant to permanently split their trading staff between multiple locations for business reasons. For example, a firm that separates its trading staff could suffer losses in productivity, since traders could lose the immediate access to market information and institutional knowledge that is gained from the concentration of traders on a single trading floor.

Similarly, all six firms that we spoke with have been working to integrate pandemic planning into their business continuity plans. For example, several of these firms have established internal committees or task forces to oversee their continuity planning for a pandemic. These internal committees have developed relationships with the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC) as well as local public health authorities and have consulted with medical experts. Moreover, these firms have joined other market participants and financial regulators at numerous meetings and tabletop exercises since late 2005 for pandemic planning. Firm officials noted that pandemic planning involves new considerations and scenarios that had not been part of traditional business continuity planning. For example, traditional plans would address the loss of facilities but not loss of staff; as a result, business continuity plans needed to be modified for a pandemic to deal with the potential reduction in staff able to work during the weeks, or even months, of a pandemic outbreak.

Although Addressing Financial Market Telecommunications Vulnerabilities Remains Challenging, Efforts to Improve the Resiliency Are Continuing

Financial market participants, in conjunction with regulators and other organizations, have made various efforts to improve the overall resiliency of the financial sector. Their actions include industry-wide connectivity testing from backup locations, expert physical security assessments of selected financial market organizations, and exercises of various disaster scenarios that include financial market participants. Financial regulators also have been assisting and promoting the creation of regional coalitions that allow financial market participants to obtain information from and interact with government and law enforcement bodies during actual disasters. Although efforts to further improve the resiliency of the telecommunications infrastructure have identified additional challenges, public and private groups continue to work together to find potential solutions, including developing ways to allow organizations to map the physical routing of their circuits and analyzing how increased teleworking during a pandemic might increase demands on telecommunications network capacity.

Financial Market Participants Involved in Various Testing and Information Sharing Efforts

To provide assurance that securities market participants can perform critical activities in the event of a disaster, industry organizations have continued to conduct an annual industry-wide connectivity test. The Securities Industry Association (SIA), together with the Bond Market Association, the Futures Industry Association and the Financial Information Forum led a test on October 14, 2006, the second year for this industry-wide effort.[11] The objectives of the test were to (1) exercise and verify the ability of market participants to operate through an emergency using backup sites, recovery facilities, and backup communications capabilities across the industry; and (2) provide participants with an opportunity to exercise and check the ability of their backup sites to successfully transmit and receive communications between the backup sites of other market participants. More than 250 organizations, including broker-dealers, markets, service bureaus, and industry utilities participated, with test participants representing more than 80 percent of normal market volume. In addition, new test components were added to the 2006 test, such as money markets and payment system processors. Test results showed a 95 percent success rate overall for successful test connections. According to association officials who assisted with the test, none of the participating exchanges or firms experienced any significant complications and when problems did arise, most were resolved quickly, allowing the test orders to be placed and processed. According to a Bond Market Association official, the test was very successful and it gave them confidence that all facets of the industry would be able to operate effectively during emergencies. Some of the preliminary lessons learned from the 2006 test are that while industry participants have been adept at resolving technical issues related to market performance when they occur, firms still need to regularly and frequently test their backup connections to market entities. Furthermore, firms and market entities must ensure that they can reach employees with key technical knowledge during emergencies.

In addition to tests within the financial markets community, cross-sector exercises have helped provide an important perspective on interdependencies across industries and how those dependencies can affect businesses' resiliency. Officials from Treasury and representatives of selected financial markets participated in two such efforts conducted by DHS. These tests—TOPOFF 3 (top officials) and Cyberstorm—were

[11]As of November 2006, SIA and the Bond Market Association merged to form an organization known as the Securities Industry and Financial Markets Association.

tabletop exercises, meant to create lifelike scenarios of disasters that force participants to look at the effect of cross-sector dependency (or interdependencies) in such catastrophes.[12] In addition to participating in these tests, SIA and the Bond Market Association used TOPOFF 3 to test their crisis communications tools and techniques—the industry's emergency alert systems that notify participants to convene and join a series of conference calls. The purpose of the conference calls is to evaluate the condition of the firms on Wall Street, relate that status to regulatory bodies that would be considering early market closings or other measures to deal with a crisis, and then transmit those instructions back to the individual firms. SIA officials reported that the tests were successful and served to identify areas in which improvements were needed, such as ensuring that all contact numbers were up-to-date and making sure that the timing, length, and sequence of calls were realistic. According to Treasury officials, they have also sponsored several exercises for the financial services sector, including some that focus on avian flu. These have been conducted with financial institution and local government representatives in various locations around the country.

In addition to national cross-sector exercises, DHS has been assisting individual firms and organizations by conducting on-site physical security assessments of various financial market organizations. Members of the Risk Management Division at DHS conduct the assessments, which include a review of an organization's facility and physical security measures such as surveillance, perimeter, and intrusion technologies. DHS prepares a group of reports that vary by security classification and provides them to the organizations with their findings and recommendations. DHS performed 19 of these assessments from fiscal years 2003 through 2006, with 21 planned for fiscal year 2007. Locations included primary facilities in multiple urban locations, as well as several key remote backup centers across the country.

[12]In 1999, Congress mandated that the departments of State and Justice conduct a series of challenging, role-playing exercises involving the senior federal, state, and local officials who would direct crisis management and consequence management response to an actual weapons of mass destruction (WMD) attack. The resulting exercises—TOPOFF (top officials), which were first conducted in 2000, are a national-level domestic and international exercise series designed to produce a more effective, coordinated, global response to WMD terrorism. This requirement is in House Report 105-825 (Oct. 19, 1998), Making Omnibus Consolidated and Emergency Supplemental Appropriations for Fiscal Year 1999.

Financial regulators also have been promoting regional coalitions to improve information sharing and response during disasters. Financial market participants have formed coalitions in cities and across wider areas such as states that allow financial market organizations to obtain information from local government, law enforcement, and other first responder organizations during actual disasters. The financial sector in Chicago formed the first of these coalitions, known as ChicagoFIRST, which sends representatives to the local emergency response command center in the event of a disaster affecting that city. This allows the ChicagoFIRST representatives to obtain accurate and timely information about what actions governmental and other bodies are taking during the event. The representatives then share the information with financial market organizations to better allow them to take appropriate actions. Coalitions also can facilitate other information-sharing efforts. For example, in July 2004, ChicagoFIRST, the City of Chicago's Office of Emergency Management and Communications, and Treasury conducted a tabletop exercise for the local financial sector. The exercise provided an opportunity for Chicago's financial community and federal, state, and local government officials to practice crisis response protocols to simulated emergency scenarios. Based on the success of the ChicagoFIRST model, Treasury published a handbook to guide such efforts in December 2004.[13] As of January 2006, the cities of Los Angeles, San Francisco, and Minneapolis and the State of Florida formed similar local collaborative efforts.

Financial market organizations also have participated in other information-sharing forums and benefited from federal dissemination of information and analyses. To assist in infrastructure protection issues, the Financial and Banking Information Infrastructure Committee (FBIIC), which includes representatives from a broad range of financial regulatory agencies, meets regularly to improve coordination and communication among financial regulators and enhance the resiliency of the financial

[13]Treasury, *Improving Business Continuity in the Financial Services Sector: A Model for Starting Regional Coalitions* (Washington, D.C.: Dec. 2004). This handbook was a collaborative effort, funded by Treasury, and co-authored by BITS, The Boston Consulting Group, and ChicagoFIRST.

sector.[14] In addition, FSSCC, which includes representatives of the financial trade associations and other entities, provides one mechanism for sharing information relating to infrastructure protection among financial market participants. FSSCC works to help reinforce the financial services sector's resilience against terrorist attacks and other threats to the nation's financial infrastructure. Formed in 2002, FSSCC acts as the private sector council that assists Treasury and DHS in addressing critical infrastructure protection issues within the banking and finance sector. FSSCC has published reports summarizing best practices and lessons learned for issues of common concern to the industry at large. Members of FSSCC also meet periodically with the financial regulators to share information about common concerns and challenges. Financial market organizations also have received consolidated information through other federal sources. For example, the Financial Services Information Sharing and Analysis Center (FS/ISAC) consolidates threat information for the sector. The financial services sector established FS/ISAC—and Treasury sponsored it—to encourage the sharing of information on physical and cyber security threats between the public and private sectors to protect critical infrastructure.[15] Between 2004 and 2005, FS/ISAC's membership grew more than 200 percent, to more than 1,800 member-organizations that receive alerts and other information directly and another 7,000 organizations that receive such information via an industry association. The alerts and information now reach 34 percent of the industry. FS/ISAC also conducts threat intelligence conference calls at the unclassified level every 2 weeks for members, with input from DHS. Treasury similarly hosts a similar biweekly threat conference call with representatives of the financial regulators and DHS. Both sets of calls discuss recent physical and cyber threats, vulnerabilities, and incidents.

[14]FBICC members include Commodity Futures Trading Commission, Conference of State Bank Supervisors, Farm Credit Administration, Federal Deposit Insurance Corporation, Federal Housing Finance Board, Federal Reserve Bank of New York, Federal Reserve Board, National Association of Insurance Commissioners, National Association of State Credit Union Supervisors, National Credit Union Administration, North American Securities Administrators Association, OCC, Office of Federal Housing Enterprise Oversight, Office of Thrift Supervision, SEC, Securities Investor Protection Corporation, and Treasury.

[15]Specifically, FS/ISAC was established in response to Presidential Directive 63 (1998). That directive—which has since been superseded by 2003 Homeland Security Presidential Directive 7—mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure.

The potential threat of a pandemic is another area in which regulators and market participants are working together to share information and increase overall preparedness. FBIIC created a working group to address pandemic flu issues that has been holding meetings among both FBIIC and FSSCC members. Treasury representatives also have participated in several working groups established by the Homeland Security Council to address pandemic flu issues. In addition, FSSCC issued a statement and issue paper on preparations for avian flu to provide guidance for financial institutions considering how to prepare for the potential of a serious influenza epidemic. The paper presents 31 key issues that financial institutions might consider in developing their plans. Some examples of the issues include the identification of critical operations (those needed for weeks or months, not days); methods of splitting and segregating staff; expanded use of tele- and videoconferencing; and coordination with local emergency management and public health organizations. In addition to publishing the statement, FSSCC formed an Infectious Disease Forum that is being led by the SIA on FSSCC's behalf. The group meets quarterly, including joint sessions with a similar pandemic working group run by federal regulators. The forum provides a venue for FSSCC members that have active avian flu working groups or are currently conducting research on this issue to collaborate and share information to prepare for a possible influenza pandemic or other infectious disease outbreak. FSSCC also provides additional information on pandemic issues on its website. Lastly, several US financial services firms participated in a recent 6-week, market wide pandemic exercise in the United Kingdom. The exercise ran in October and November 2006, with 70 organizations and about 3,500 staff from across the financial sector taking part. Officials from the U.S. federal regulator community provided input into the scenario planning of the event. UK officials who ran the exercise stated in the summary report that an important next step would be to work with their international regulatory partners to ensure cross-border regulatory coordination—and thus that global financial markets will be able to continue operating in a pandemic.

Various Activities Were Under Way to Improve Resiliency of Telecommunications, but Identifying Clear Solutions Remains Difficult

Since the 2001 attacks, financial regulators, market participants, and other organizations have engaged in various efforts to improve the resiliency of the telecommunications infrastructure upon which the markets depend, but clear resolutions to the various challenges have proved difficult to identify. As we reported in 2003, September 11 showed that such events can have significant effects on the telecommunications services that support the U.S. financial markets. Although some financial market participants attempted to ensure that they would not lose

telecommunications service by contracting with more than one telecommunications carrier, the attacks revealed that multiple carriers' lines and circuits often traversed the same physical paths or relied on the same switching offices and thus were susceptible to damage from the same event. One way that financial markets organizations have attempted to address this problem is by exploring the feasibility of mapping the physical paths that individual organizations' telecommunications circuits follow.

However, completing such analyses has proved very time-consuming and expensive. According to a 2004 report by the President's National Security Telecommunications Advisory Committee (NSTAC), carriers would have to use labor-intensive, manual processes to ensure route diversity and monitor that condition on an ongoing basis. The NSTAC report further stated that guaranteeing that circuit routes would not be changed could make an organization's service less reliable because its circuits could lose the benefit of technologies that automatically reroute circuits in the event of facility failures. To assess the feasibility of mapping physical circuit routing, the Federal Reserve participated in the National Diversity Assurance Initiative—a joint project between the Federal Reserve and various telecommunications carriers—that the Alliance for Telecommunications Industry Solutions (ATIS) conducted.[16] After doing an initial assessment of the circuits, the initiative decided that conducting an end-to-end multi-carrier assessment of telecommunications circuits could only be conducted manually, a very labor and cost intensive process. The members of the initiative concluded that attempting such an analysis for large numbers of circuits in multiple organizations would be very difficult. As a result, the ATIS report indicated that an automated system would likely have to be developed to more efficiently track circuits across multiple carriers and make end-to-end diversity assessments and assurance feasible on any larger scale. The report recommended a small-scale follow-up effort to determine the objectives and requirements for a system that could provide end-to-end diversity assurance in a multicarrier environment. According to the report, the scoping effort should attempt to identify the high-level requirements, cost estimates, and level of effort needed to develop and implement an automated circuit assurance solution. Since this report was issued, the National Communications

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

System (NCS) within DHS, which is responsible for administering the federal national security and emergency preparedness telecommunications programs, has agreed to lead an effort—the Diversity Assurance Analysis—to explore the potential for developing automated solutions to the circuit diversity problem.

Telecommunications providers are also attempting to improve the resiliency of the infrastructure upon which the financial markets depend. As we previously reported, much of the disruption to voice and data communications services throughout lower Manhattan—including the financial district—that stemmed from the 2001 attacks occurred when one of the buildings in the World Trade Center complex collapsed into an adjacent telecommunications center, which served as a major local communications hub within the public network. Since then, the provider that operates this facility has been rebuilding portions that were damaged or lost in the attacks, using designs that provide greater resiliency and redundancy to their infrastructure in lower Manhattan. For example, the provider has reinforced the storage area for generator fuel with a protective wall and now routes the fuel through concrete-lined conduits. The provider also has updated parts of its network to use more resilient advanced switches and used more fiber-optic cables, which are smaller but can carry more message traffic.

Financial market regulators and participants also have become concerned about the potential impact of a pandemic on telecommunications resiliency. As many financial market organizations have begun considering how best to ensure business continuity in during a disease outbreak, many (including some of the broker-dealers that we contacted) considered having large numbers of their employees telecommute. However, concerns have been raised about whether the existing telecommunications networks would have adequate capacity for absorbing the additional data and voice communications traffic. For example, all the calls that originate in individual neighborhoods usually must go through a single set of switches before reaching the larger-capacity and more redundant telecommunications network. It is not known whether the lines and switches serving individual neighborhoods or areas would have sufficient capacity, particularly since more people overall may be home during a pandemic, as a result of school or workplace closings. For example, in a June 2006 testimony before Congress, an FSSCC official stated that the financial markets community did not have enough information to determine whether the nation's telecommunications infrastructure could support a rapid and explosive increase in users on specific networks. Consequently, FSSCC recommended that NSTAC be asked to research this

issue and identify any recommendations to ensure that the telecommunications sector's networks were robust enough to meet other sectors' demands during such a potentially stressful time.

In addition, in November 2006, FSSCC and telecommunications carriers agreed to collaborate on an NCS study about the potential impacts of a pandemic on telecommunications infrastructure. The study will focus on the technical feasibility of national policy and business continuity planning related to telecommuting in response to the pandemic influenza threat. According to an NCS official, previously completed models on this issue indicate that sufficient bandwidth to accommodate increased traffic during a pandemic appears to exist on a national level, but problems could be experienced in the individual neighborhood or commercial area connections points, which are the "first mile" or "last mile" of the connection to the national system. The financial market participants from FSSCC will assist NCS by contributing their business continuity telecommuting plans and estimated traffic load during a pandemic. These plans will be used in examining potential access network issues for the financial community and serve as an example for other industries in predicting the potential change in traffic on access networks. Telecommunications carriers will provide estimates of potential surge traffic from the general public during a pandemic using related historical data (e.g., snowstorms). The financial community anticipates benefits from this study would include recommendations on mitigation measures that could be implemented either in advance or in real time for the various impact levels possibly encountered during a pandemic.

Financial Market Regulators Have Acted to Improve the Readiness of the Financial Sector and Plan to Address Remaining Challenges

Federal financial regulators have taken a variety of steps to strengthen the ability of the U.S. securities markets to recover from a wide-scale disaster. In 2003, regulators jointly issued business continuity guidance to strengthen the resiliency of key organizations and firms that clear and settle transactions in critical financial markets. The regulators expect these organizations to be able to recover and resume their clearing and settlement activities on the same business day on which a wide-scale disruption occurs. Since 2003, regulators have conducted examinations and determined that all of these organizations and firms have substantially implemented this guidance or will soon do so. SEC and banking regulators also have been reviewing the planning that organizations that participate in the securities markets are doing to address pandemics, but have not other actions that could improve readiness. SEC has issued expectations that markets be prepared to resume trading promptly after disasters, and its staff have taken steps to assure themselves that large market

participants have taken sufficient actions to increase the likelihood that U.S. markets would resume trading. SEC staff also plan to do more focused reviews of broker-dealer trading readiness. SEC also has taken actions to improve the ARP program that it uses to oversee systems operations issues at the markets and clearing organizations, including increasing staffing levels and expertise and preparing a rule mandating compliance with the ARP program's tenets for which it expects to seek approval during 2007.

Regulators Have Taken Additional Steps to Reduce Likelihood of Disruptions to Clearance and Settlement Activities

Since 2003, federal financial regulators have worked in a coordinated manner to assess and improve the resiliency of the U.S. securities markets with respect to clearance and settlement activities. As we noted in our last report, in April 2003, SEC, the Federal Reserve, and OCC jointly issued the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (Sound Practices). [17] The Sound Practices paper establishes business continuity expectations for the clearance and settlement activities of organizations that support critical financial markets. These organizations include the core clearing and settlement entities that process securities transactions (core organizations) and firms that play a significant role in critical financial markets (significant firms)—generally defined as those firms whose participation in the markets results in their consistently clearing or settling at least 5 percent of the value of the transactions in any of the product markets specified in the paper.[18] The agencies expect these organizations must be able to recover and resume their clearing and settlement activities on the same business day on which a wide-scale disruption occurs.[19] To achieve this goal, the organizations would maintain geographically dispersed facilities and resources and routinely use or test their recovery and resumption arrangements to ensure their effectiveness.

Since issuing the paper, regulators have been conducting examinations of the organizations subject to these practices and have determined that

[17]68 Fed. Reg. 17809, 17810 (2003).

[18]"Core clearing and settlement organizations" consists of government or private sector entities that provide clearing and settlement services that are integral to a critical market. Among the specific product markets included in the paper are those for government and corporate securities, commercial paper, foreign exchange, and others.

[19]Core clearing and settlement organizations should strive to recover these activities within 2 hours of a disastrous event, and significant firms should strive to recover these activities within 4 hours.

those organizations have substantially achieved the capabilities envisioned in the Sound Practices paper or soon will do so. Specifically, SEC, the Federal Reserve, and OCC have reviewed firms' primary and backup data center arrangements, the amount of time that it takes firms to recover their operations at their backup sites and firms' tests of their backup arrangements. In an April 2006 report to Congress, the regulators reported that the core organizations all have data and operations centers that are geographically remote from their primary sites.[20] Regulators also noted that several of these organizations share or periodically shift their operations between their primary and backup sites; this practice prepares them to continue their operations in the event of a disruption at either location. Although the significant firms initially were expected to be capable of resuming their clearing operations within the time frames in the Sound Practices paper, regulators extended this deadline for some firms because of the work and costs associated with implementing these practices. For example, when the practices were issued in 2003, one firm had just completed a new data center only several miles away from its primary site; as a result, this firm requested—and was granted—additional time to establish a geographically remote data center. According to the representatives of regulators and firms with whom we spoke, all significant firms likely will have sufficiently dispersed sites capable of conducting critical clearing activities by March 2007 and thus will have substantially achieved the practices. In contrast with the situation existing in 2001, the regulators conclude that by increasing the geographic diversity of their operating locations, the core organizations and significant firms significantly have increased the likelihood that critical financial markets will be able to recover clearing and settlement activities fairly rapidly after a wide-scale disruption.

With most firms having sites allowing them to recover their operations within the Sound Practices time frames, regulators are expecting firms to conduct meaningful tests of these capabilities in the near term. In January 2006, SEC, the Federal Reserve, and OCC issued a detailed letter to all core organizations and significant firms, outlining expectations for the testing strategies that organizations and firms should use to verify their

[20]The Federal Reserve, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Joint Report on Efforts of the Private Sector to Implement the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (Washington, D.C.: April 2006).

implementation of the Sound Practices.[21] In this letter, regulators advised organizations and firms that they should have a comprehensive and risk-based testing approach that includes routine use or testing of recovery and resumption arrangements. In addition, the significant firms should assess whether their recovery arrangements were compatible with those of the core organizations. The fundamental testing concepts included in this letter are also being incorporated into a revised version of the business continuity planning guidance that the Federal Financial Institutions Examination Council—which issues guidance developed jointly by the various depository institutions regulators—plans to issue later this year.[22]

Regulators Are Actively Addressing Pandemic Planning, but Additional Actions Could Improve Readiness

Banking and securities regulators have been working to assist market participants' pandemic planning efforts, but have not taken other actions that could better assure that market participants adequately prepare for a pandemic. For example, the New York Stock Exchange (NYSE), which is a self-regulatory organization (SRO) that oversees its broker-dealer members, issued an information memorandum to provide guidance to member organizations about how to assess whether their business continuity and contingency plans would be suitable for a prolonged, widespread public health emergency.[23] In a letter sent to securities exchanges and clearing organizations, the Acting Director of SEC's Market Regulation Division noted that these organizations should promote planning and preparations to keep the markets operating during a pandemic. This letter notes that while securities exchanges and clearing organizations already have extensive business continuity programs, such plans are usually designed to address a discrete event and therefore may prove inadequate to address the potentially long-lasting impact of a pandemic, which could include multiple waves of outbreaks lasting 6 to 8 weeks. It also notes that federal, state, or local governments may take actions, such as quarantines, that may make it more difficult to maintain critical operations using remote backup sites. Although acknowledging

[21]The Federal Reserve, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, *Re: Assessing the Implementation of the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System by Core Clearing and Settlement Organizations and Firms that Play Significant Roles in Critical Markets* (Washington, D.C.: January 2006).

[22]The regulators of federally insured depository institutions jointly develop and implement FFIEC guidance to ensure consistency of practices among depository institutions.

[23]NYSE Information Memo Number 06-30, May 2, 2006.

that developing such plans would be difficult, the letter notes that such planning is necessary for organizations to analyze options and prepare for how the markets may function if confronted with an outbreak. In addition to this letter, SEC staff also have been speaking at forums such as conferences and meetings with market participants—industry trade associations, FSSCC—to share information about pandemic issues. Furthermore, SEC staff told us that they have also begun to review pandemic planning issues during inspections of exchanges, electronic markets, clearing organizations, and broker-dealers. In a joint notice from the regulators that oversee banks and thrifts, the agencies indicated that their institutions should review the U.S. government's national pandemic strategy to consider what actions may be appropriate for their particular situation, and whether such actions should be included in their event response and contingency strategies. The bank regulators noted that financial institutions with a global presence and those considered critical to the financial system may have greater preparation and response challenges than those of other financial institutions. Bank regulation officials told us that they have also begun reviewing pandemic planning in the context of their ongoing supervisory activities. Lastly, SEC officials told us that they are beginning to work with the Securities Industry and Financial Markets Association to plan for a 4-week exercise beginning in September 2007 that will be modeled after the exercise conducted in the United Kingdom (discussed earlier in this report). This exercise will test how ready U.S. securities firms are to operate during a future flu pandemic.

Although regulators have been actively addressing pandemic issues, they have not taken some additional actions that could improve readiness within the financial markets. For example, SEC and banking regulator staff told us that they are speaking about the need for financial institutions to prepare for a potential pandemic and they have issued general statements indicating that market participants should develop plans and provided issues to consider. However, none of these issuances specifically directed market participants to prepare plans likely to be effective in the midst of even the most severe outbreaks, which can result in significant levels of illness, deaths, transportation shutdowns, or constrained telecommunications capabilities. SEC staff told us that developing such plans is complicated. For example, important information for the effectiveness of the plans is not currently fully known, such as when and where outbreaks will occur, how virulent they will be, and how quickly they will spread. In addition, the actions that governments may take in response to a pandemic also are not certain, such as whether quarantines would be imposed or schools would be closed. As a result, the SEC staff

said that financial market organizations will need to have flexible plans that accommodate various scenarios and actions. Regulatory staff also noted that the U.S. government has yet to establish dates by which other sectors should have complete plans. Given that state and local governments, or organizations in power, telecommunications, transportation, or other sectors upon which the financial markets depend may take a range of actions, such as quarantines, that could affect the viability of financial market organizations' pandemic plans, clear expectations from regulators that financial market organizations' plans should address such scenarios would provide greater assurance that all critical organizations and key market participants prepare plans that are sufficiently robust.[24]

Banking and securities regulators also have not set dates by which market organizations would be expected to have prepared at least an initial formal business continuity plan intended to ensure that critical operations can continue during a pandemic. Given that a pandemic could begin at any time, having complete formal plans in place beforehand would better ensure that financial market organizations could respond immediately. Completing such formal plans would allow exchanges, electronic markets, clearing organizations, broker-dealers, and banks to identify and begin acquiring any needed additional resources, such as medical supplies or computer hardware. In addition, completing initial plans soon would ensure the plans are appropriately approved by organization management and allow organizations to begin training employees and preparing communications for customers about possible changes in operating procedures during a pandemic.

As part of preparing plans for pandemics, market participants have indicated that regulators should specify the types of regulatory relief that might be provided. Several of the broker-dealers with whom we spoke told us that they anticipated needing some form of regulatory relief in a pandemic situation. For example, broker-dealer staff likely would be working from home during a pandemic due to health concerns, and as a result, regulators might have to grant some relief from requirements that broker-dealer personnel be directly supervised. NASD, which is an SRO for its broker-dealer members, issued a notice seeking their input regarding what specific, short-term regulatory relief might be necessary to

[24]GAO has ongoing work evaluating federal, state, and local governmental pandemic response plans.

maintain market stability while still providing sufficient protections for investors.[25] In providing comments to NASD, two trade associations for securities noted that such relief might be necessary to give broker-dealers the flexibility to operate when a large number of employees were not in their regular work space, either because they were sick, caring for others, or afraid to come into the office. While some employees might be able to work from nonregular locations, the trade associations noted that the requirement to register new temporary offices as new branch office locations may have to be suspended as was done after the September 2001 attacks and Hurricane Katrina.[26] Another area in which relief might be needed would involve providing additional time for broker-dealers to submit personnel registrations and for those staff to fulfill continuing education requirements. Similarly, the associations noted that the time for conducting normal supervisory reviews should be extended during a pandemic because the personnel who perform such reviews were likely to be needed to help their firms in actual business activities. According to their comment letter, regulatory relief would be necessary no matter what method of operation a broker-dealer chooses because the number of absent employees likely would cause difficulties in promptly settling transactions and delaying many other activities. The associations urge the regulators to cooperate in a multiregulator process that coordinates granting relief as well as proposing that any trigger (such as a certain percentage infection rate that the Centers for Disease Control would declare) for the commencement of relief should occur at the same time across the markets.

After collecting the information on what types and under what circumstances that regulatory relief may be needed, NASD officials indicated that they intend to work with SEC and other SROs to determine what relief may be appropriate. Similarly, to appropriately respond to such anticipated requests for regulatory relief, NYSE has filed a draft rule proposal with SEC seeking more authority to grant exemptive regulatory relief in the event of a pandemic. For example, under the proposed rule, NYSE may waive or extend the time otherwise applicable for complying with examination, training, or continuing education requirements.

[25]NASD*: Request for Comment: Pandemic Regulatory Relief*, Notice to Members 06-31, (Washington, D.C.: June 2006).

[26]The Bond Market Association and the Securities Industry Association, *Re: NASD Notice to Members 06-31*, (Sept. 15, 2006).

Although willing to consider regulatory relief, SEC staff indicated that market participants should not expect wide-scale waivers of important securities regulatory requirements. Although SEC staff told us that they recognize that some form of regulatory relief would most likely be part of the process of enabling the financial system to keep operating under the trying conditions of a pandemic, they also noted that such relief should be one of the last stages in continuity planning and preparation, not the first. Instead, they said that market participants should develop plans and capabilities for continuing operations during a pandemic that also would allow organizations to materially comply with important securities regulations. These areas included ensuring that broker-dealer personnel were properly supervised, necessary records prepared, and price transparency for securities maintained.

Regulators Have Worked to Ensure That Trading Activities Will Resume After a Disaster, and Plan to Examine Broker-Dealer Readiness More Fully

Although broker-dealers are not required to be able to resume operations after disasters, securities regulators have issued some guidance and conducted some assessments of firms' readiness to trade. As noted in our last report, SEC issued a policy statement in 2003 that established business continuity guidelines for the exchanges and electronic markets that match buy and sell orders for securities.[27] This guidance expects these exchanges and markets to develop business continuity plans and be prepared to resume trading on the next business day following a wide-scale disaster. SEC examiners from the ARP program have been conducting examinations of the various markets subject to this policy statement to ensure that these entities had sufficient capabilities to conduct operations even if a wide-scale disaster damaged or rendered their primary operating sites inaccessible. Specifically, these SEC staff have determined that the two largest markets have implemented business continuity capabilities that likely would allow them to resume trading activities within one day of a disaster.

Although SEC issued some guidance addressing business continuity expectations for exchanges and other trading venues, the firms that trade on U.S. markets are not required to ensure that they can resume operations after disasters. According to SEC officials, no provisions in the securities laws explicitly require that firms conducting securities activities be operational under all circumstances and resuming operations in the

[27]Business Continuity Planning for Trading Markets, SEC Exchange Act Release No. 48545 (Sept. 25, 2003), published in 68 Fed. Reg. 56656, 56657 (Oct 1, 2003) (policy statement).

aftermath of a disaster would be a business decision left to the management of individual firms. Nevertheless, NYSE and NASD, which together oversee the majority of broker-dealers operating on U.S. markets, have issued rules that establish business continuity expectations for their members.[28] These rules require broker-dealers to develop business continuity plans that address various areas, including data backup and recovery, and alternate means for communicating with customers. Although these rules do not require firms to be capable of resuming operations in the event of a disaster, NYSE staff that conduct reviews of their member firms told us that many firms are attempting to implement such capabilities for their own business reasons. If a firm were unable to develop sufficiently robust capabilities that would allow it to resume trading, the NYSE and NASD rules require that such firms must, at a minimum, have the capability to ensure that its customers would have access to their funds and securities. For example, NASD staff who oversee their member firms told us that some firms provide customers with contact information for their clearing organizations on customer account statements and firm Web sites. Based on reviews done by their examiners, NYSE and NASD officials reported that most of their member firms have implemented these business continuity planning rules, although larger firms generally were more likely to be compliant than smaller firms.

SEC has undertaken some assessments of the readiness of broker-dealers to resume trading in the event of disasters and plans to conduct more specific examinations of broker-dealers' capabilities in the future. In response to the recommendation in our last report that SEC fully analyze the readiness of the securities markets to recover from major disruptions, SEC staff told us that they have taken various actions to assess the ability of broker-dealers to resume trading promptly after disasters. Staff from SEC's Market Regulation Division and Office of Compliance, Inspections, and Examinations told us that, in consultation with the other federal agencies and local emergency management officials in New York and Chicago, they have considered how a wide range of disaster scenarios would affect the securities markets. These scenarios include both a variety of man-made threats (including chemical, biological, and radiological terrorist events) and natural disasters (including a severe hurricane or a pandemic). According to SEC, the likely impact of these events will vary from scenario to scenario and from organization to organization. They also have had discussions with key broker-dealer market participants about

[28]NYSE Rule 446; NASD Rule 3510 and 3520.

their capabilities and plans for overcoming various disasters. For example, after publication of the Sound Practices paper, SEC staff conducted an analysis of the major firms to ascertain their willingness and ability to continue to trade in the event of a wide-scale disruption. SEC staff told us that these firms all expressed a commitment to continue to operate and have allocated substantial resources to enhance their resilience sufficiently to permit them to trade. Accordingly, SEC staff believe that market participants have increased their resiliency since September 11 and that based on this work sufficient numbers of firms and staff likely would be able to operate from various locations to allow U.S. markets to resume trading when appropriate.

During discussions we had with SEC staff as part of this review, staff responsible for conducting broker-dealer examinations told us that their efforts since the 2001 attacks have been more focused on ensuring that firms were improving their capabilities for recovering their clearance and settlement activities, as required under the Sound Practices paper. However, based on our inquiries about trading readiness, SEC staff agreed that they could take further steps to assess broker-dealers capabilities in this regard. As a result, they developed an expanded examination module to obtain more detailed information on firms' business continuity capabilities related to trading activities and have made this part of the existing examination guidance for the SEC examiners. SEC officials told us that they expect to use this expanded guidance in the applicable broker-dealer examinations beginning with the 2007 cycle.

SEC Has Made Various Improvements to the ARP Program

Since 2004, SEC has implemented various improvements to its ARP program, which oversees operations of automated and information technology systems at exchanges, clearing organizations, and electronic communications networks. In response to our past recommendations to SEC to expand the level of staffing and resources committed to the ARP program, SEC hired four new staff members during 2005, increasing the program's staffing from 9 to 13. In addition, in response to our recommendation that SEC increase its overall technical expertise, all four of these newly hired staff have at least master-level degrees in information security-related fields. SEC has obtained funding to establish its own information security laboratory and is acquiring hardware that the agency can use to test systems and equipment being used by market participants and to help ARP staff learn about information security vulnerabilities and protection practices. To further improve the technical sophistication of the ARP examinations, SEC also began contracting with an information technology consulting firm to supplement its staff on information security

reviews of the entities the ARP program oversees. During the last 2 years, staff from this consulting firm accompanied SEC staff on several reviews of the larger organizations, and our review of the reports that were prepared indicated that this firm's assistance has helped SEC expand the range and breadth of issues that it reviewed during those examinations.

In response to our prior concerns that SEC was not examining important market organizations frequently, staff responsible for the ARP program have changed their practices to increase how often they will conduct reviews of the more critical organizations. While we had previously reported that the intervals between examinations for many of the critical organizations had been as much as 3 years, ARP staff, since implementing the new practice, have been annually reviewing the organizations they consider most important. Our analysis of ARP report data from fiscal years 2003 through 2006 confirmed that the critical organizations under SEC's jurisdiction were being reviewed at least annually.[29] Furthermore, we reviewed the reports from the ARP examinations conducted between March 2004 and May 2006, and they indicate that the ARP staff generally were addressing all the key areas, including telecommunications, physical security, information security, and business continuity planning, during the examinations they have conducted. For example, we reported in 2003 that few of the ARP program examinations addressed physical security issues. During this period, we found that several of the organizations had hired an external consultant to review their physical security adequacy as a result of prior ARP staff recommendations. In addition, while we reported that SEC staff sometimes had problems getting organizations to implement ARP staff recommendations, our review of the latest examinations indicated that the organizations that SEC examined were implementing the ARP staffs' recommendations appropriately. For example, in 6 of the 8 exams conducted in 2005, the examined organization had since taken actions sufficient to close all recommendations made previously.

Although SEC appears to be getting adequate cooperation from the entities that it reviews as part of the ARP program, SEC currently administers the ARP program under policy statements on a voluntary basis. Consistent with one of our prior recommendations, staff in SEC's

[29]Of the seven organizations that we considered critical to the overall functioning of the markets for purposes of this report, five are subject to the ARP program. The other two organizations are overseen by the Federal Reserve.

Market Regulation Division told us that they continue to make progress in obtaining approval of a rule that will make adherence to the ARP program mandatory for affected organizations. SEC staff told us they have drafted a rule that will allow them to cite firms for rule violations if they fail to adhere to the expectations of the ARP program and assess penalties similar to other SEC requirements. The draft rule has been undergoing a series of internal reviews and staff expect to present it to the SEC Commissioners for issuance in spring 2007. Given the importance of the activities that the ARP program oversees to the U.S. securities markets, we continue to support making ARP a rule-based program to better assure that the SEC staff have the necessary leverage to ensure compliance with any recommendations they deem necessary for the continued functioning of the markets.

Conclusions

Based on the series of reviews we conducted, the financial regulators and market participants have made considerable progress in the more than 5 years that have passed since September 11, 2001, in improving the security and resiliency of the U.S. securities markets against potential attacks and other disruptions. The critical exchanges and clearing organizations all have implemented increased physical security measures to reduce their vulnerability to physical attacks and reduced the vulnerability of their key information systems and networks to cyber threats. Most significantly, all of the organizations now have the capability to conduct their operations from backup sites that are at a significant geographic distance from their primary locations, a move that greatly reduces their vulnerability to even wide-scale disasters that affect their primary operating locations. During this period, financial market regulators also have contributed to the increased security and resiliency of the markets by actively overseeing and encouraging market participants' efforts and by issuing guidance and conducting examinations.

Although considerable progress has been made, regulators, participants, and others remain appropriately focused on various ongoing challenges. The need to assess and incrementally improve physical and information security measures remains constant as techniques for both attacking and protecting the critical assets of the financial markets will continue to evolve. With functioning telecommunications systems being vital to the markets' ability to operate, efforts by regulators, market participants, telecommunications providers, and other government bodies to improve the availability and resiliency of this key infrastructure are critical. Finally, although SEC staff have assured themselves that key broker-dealers also were acting to improve their resiliency, we are encouraged by

SEC's recent plans to focus even greater attention on these efforts to ensure that sufficient numbers of such firms will be available to trade following future disasters.

Although banking and securities regulators have taken various actions to help the financial markets prepare for and respond to an influenza pandemic, additional actions could further improve the readiness of the financial markets to withstand this threat. To their credit, financial market organizations have begun considering a range of issues related to pandemics and are working with others to improve readiness, such as by assisting with analyses of the capacity of the telecommunications infrastructure with relevant government agencies. However, at the time we visited them we found that few of the critical financial market organizations had completed the development of formal plans specifying the actions they would take and the capabilities and resources they would need to be able to continue their critical operations if significant numbers of their staff were ill or unavailable during a pandemic.

When faced with the recognition that attacks or natural disasters could significantly disrupt market operations, financial regulators responded by issuing guidance and expectations—in the Sound Practices paper and in other policy statements—that specified the actions that market participants should take and set deadlines by which these actions should be taken. Although a pandemic could similarly disrupt financial organizations' ability to operate, the regulators, although actively addressing pandemic issues, have not taken similar actions. Regulators indicated they are advising market participants in meetings and other forums to prepare plans that address the impacts of even a severe pandemic; however, these regulators have not issued any formal statements of these specific expectations. Without such official expectations, market participants may not adequately prepare plans that are sufficiently robust to address the more serious scenarios, which could include widespread illnesses, deaths, transportation bans, or telecommunications bottlenecks. In addition, the regulators have not set a date by which financial organizations should have their pandemic plans completed. Having plans that fully meet regulatory expectations in place before an outbreak would allow organizations to provide training to their employees and conduct tests and exercises of their plans that could provide valuable insights into how to further improve their readiness. Given that the severity of pandemic and the potential responses that governments or other organizations may take can vary, effective business continuity plans will have to be flexible by including a range of measures that financial market organizations can implement depending on

circumstances, and these plans will have to be updated continually as new information arrives. Having such plans in place soon would help organizations to identify any additional resources needed, obtain the appropriate management approvals, and prepare their staff and customers for changes in how an organization may operate during a pandemic. While governmental bodies have not taken similar actions for other key sectors of the U.S. economy, such action by regulators of the financial sector could demonstrate the leadership that the sector is known for and serve to spur other sectors to accelerate their progress as well.

Recommendation for Executive Action

To increase the likelihood that the securities markets will be able to function during a pandemic, we recommend that the Chairman, Federal Reserve; the Comptroller of the Currency; and the Chairman, SEC, consider taking additional actions to ensure that market participants adequately prepare for an outbreak, including issuing formal expectations that business continuity plans for a pandemic should include measures likely to be effective even during severe outbreaks, and setting a date by which market participants should have such plans.

Agency Comments and Our Evaluation

We provided a draft of this report to the Federal Reserve, OCC, Treasury, and SEC for their review and comment. In a letter from a Staff Director for Management, the Federal Reserve, the Comptroller of the Currency, and the Director of SEC's Market Regulation Division, these officials indicated that they shared our views on the importance of ensuring that the financial markets enhance their resiliency (see app. II). In addition, they acknowledged that we recognized that the financial markets have made significant progress in increasing their ability to withstand wide-scale disasters. Regarding our recommendation that these regulators consider taking additional actions regarding pandemic preparedness—including issuing specific instructions that organizations plan for severe pandemics and setting a date by which business continuity plans for pandemics should be completed, the officials noted that the critical organizations and key market participants subject to the Interagency Sound Practices paper are planning for a pandemic, including a severe outbreak, and identifying measures to reduce their vulnerabilities to such events. They also noted that all of these organizations have been subject to supervisory review over the past several months, and that these organizations' contingency plans generally address the four elements recommended in our report. The officials also indicate that their agencies have incorporated reviews of organizations' pandemic planning efforts into their ongoing supervision and oversight processes to ensure that the critical market organizations

are updating their plans as new information becomes available and incorporating lessons learned from market exercises. In their letter, the officials indicate that they will follow up to ensure any weaknesses in the ongoing pandemic-planning process are appropriately addressed by the organizations, and if the regulators find that organizations' efforts are lagging, they will consider taking additional actions, including those that we have suggested.

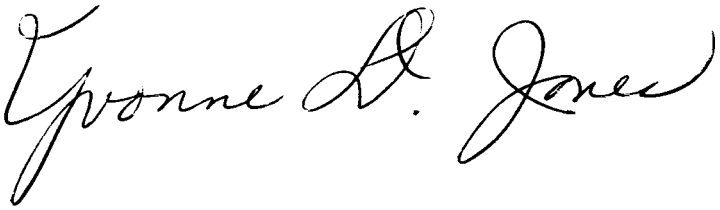
We are encouraged that the regulators plan to actively monitor the progress that critical organizations and key market participants are making to plan and prepare for a pandemic. Although the regulators maintain that organizations have prepared plans that address all expected elements, during the agency comments process we obtained the draft pandemic plan for one of the critical organizations. Based on our review, this organization's plan addressed some of the expected elements, but did not include the specific procedures that would be used to ensure that its critical operations would continue during a pandemic. The organization indicated these procedures would be described in business unit plans that were still being prepared. In addition, we recently recontacted representatives at five of the six key market participants that we had reviewed, and while most indicated that they had received sufficient instruction from regulators regarding pandemic expectations, staff at one firm told us that, although they had attended meetings with regulators on pandemic issues, they have not received any guidance on specific scenarios to plan for, such as transportation shutdowns. Because at least some organizations may not yet be fully prepared or potentially may fail to consider the potential pandemic scenarios associated with a severe outbreak, particularly if mitigating them is difficult and discourages or delays firms' willingness to fully prepare, we continue to believe that having regulators give greater consideration to providing specific instructions to market participants and setting a date for having pandemic continuity plans complete would increase the likelihood that organizations fully prepare and have adequate time to test and adjust any planned responses in advance of the outbreak of an actual pandemic.

We also received technical comments from Federal Reserve, OCC, SEC, and Treasury staff that we incorporated where appropriate.

As agreed with your offices, unless you publicly announce the contents earlier, we plan no further distribution of this report until 30 days after the date of this report. At that time, we will send copies of this report to other interested congressional committees and the Chairman, Federal Reserve;

the Comptroller of the Currency; and the Chairman, SEC. We will also make copies available to others upon request. The report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions regarding this report, please contact me at (202) 512-8678 or jonesy@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.



Yvonne Jones
Director, Financial Markets and Community Investment

List of Congressional Requesters

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

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

The Honorable Bobby L. Rush,
Chairman
The Honorable Cliff Stearns,
Ranking Minority Member
Subcommittee on Commerce, Trade,
and Consumer Protection
Committee on Energy and Commerce
House of Representatives

The Honorable Jan Schakowsky
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The objective of this report is to describe the progress that financial markets participants and regulators have made since our 2004 report in ensuring the security and resiliency of our securities markets. Specifically, we assessed (1) actions critical securities market organizations and key market participants have taken to improve their business continuity capabilities for recovering from physical or electronic attacks and the security measures they use to reduce their vulnerabilities to such events; (2) actions taken by financial market participants, telecommunications industry organizations, and others to improve the ability of participants to respond to future disasters and increase the resiliency of the telecommunications on which the markets depend; and (3) financial regulators' efforts to ensure the resiliency of the financial markets, including SEC's progress in improving its securities market organization oversight program.

To assess the actions that critical securities market organizations and key market participants took to improve their business continuity capabilities for recovering from physical or electronic attacks and the security measures they used to reduce their vulnerabilities to such events, we reviewed the actions of seven organizations whose ability to operate is critical to the overall functioning of the financial markets. To maintain the security and the confidentiality of their proprietary information, we agreed with these organizations that our report 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 how these organizations ensured they could resume operations after an attack or other disaster, we discussed their business continuity plans and capabilities with their staff and visited their facilities. We compared their plans to 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 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. When possible, we directly observed the operation of these backup sites and reviewed relevant documentation, including backup facility test results that the organizations provided.

To assess what critical organizations had done to minimize the likelihood that physical attacks would disrupt their operations, our staff that

routinely conduct physical security reviews at government agencies and private organizations conducted on-site "walkthroughs" of the critical organizations' facilities, reviewed their security policies and procedures, and met with key officials responsible for physical security to discuss these policies and procedures and compared these with guidance that the U.S. Department of Justice developed for federal buildings.[1] Based on these and other 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 determine what the seven critical organizations did to reduce the risks to their operations from electronic attacks, our information technology security staff that routinely conduct information security reviews at government agencies and private organizations assessed progress made on issues previously identified in our past reviews and visited and reviewed documentation for the critical organizations' 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 best practice or principles for electronic security.[2] 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, how they detected intrusions, and what assessments of their systems' vulnerabilities they had performed.

In addition to the critical organizations, we also obtained information from six large broker-dealers and banks that collectively represented a significant portion of trading and clearing volume on U.S. securities

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

[2]GAO, *Federal Information Systems Controls Audit Manual, Volume I: Financial Statement Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: Jan. 1999) and the Federal Financial Institutions Examination Council's *Information Systems Handbook: Volume 1* (Washington, D.C.: 1996).

markets. At these organizations, we discussed their business continuity capabilities and reviewed documents where available.

To determine how financial market participants, telecommunications industry organizations, and others improved the ability of participants to respond to future disasters and increased the resiliency of the telecommunications on which the markets depend, we reviewed documents and interviewed staff from financial market regulators, industry associations, and government agencies responsible for protecting critical infrastructure. Finally, we met with managers at a large telecommunications carrier to review how they were rebuilding local infrastructure in New York City.

To assess financial regulators' efforts to ensure the resiliency of the financial markets, including SEC's progress in improving its oversight program, we reviewed relevant regulations and guidance and interviewed officials at SEC, the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and the Department of Treasury. We also collected data on the examinations the regulators had conducted of exchanges, clearing organizations and banks, and broker-dealers and reviewed the examination reports for the examinations completed from 2004 through 2006. To assess the efforts of SROs to ensure financial market resiliency—including the New York Stock Exchange (NYSE) and NASD, which are responsible for overseeing their broker-dealer members—we reviewed SRO rules, interviewed NYSE and NASD officials, and reviewed the results of NYSE and NASD business continuity examinations of member firms. 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, the Securities Industry Association, and ChicagoFIRST—a non-profit association that addresses homeland security and emergency management issues affecting Chicago's financial institutions.

We performed our work from April 2006 to February 2007 in accordance with generally accepted government auditing standards.

Appendix II: Comments from the Federal Reserve, the Comptroller of the Currency, and the Securities and Exchange Commission

Board of Governors of the Federal Reserve System
Office of the Comptroller of the Currency
Securities and Exchange Commission

March 16, 2007

Ms. Yvonne Jones
Director, Financial Markets and Community Investment
United States Government Accountability Office
Washington, DC 20548

Dear Ms. Jones:

We appreciate the opportunity to respond to your draft report titled "Financial Markets Preparedness: Significant Progress Has Been Made, but Pandemic Planning and Other Challenges Remain," GAO-07-399. The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission (collectively the "Agencies") share the GAO's views regarding the importance of emergency preparedness of the critical financial markets. We, therefore, appreciate the GAO's recognition of the significant progress that critical financial market organizations have made to enhance their resiliency for potential wide-scale disruptions since your 2004 report.

The draft report notes that, since the last report, critical financial market organizations and other key market participants have significantly improved their ability to recover operations in the event of a wide-scale physical disaster. The draft report also notes, however, that to improve the readiness of the securities markets to withstand a potential pandemic, securities and banking regulators should consider taking various actions, including providing formal expectations that market participants' plans address even severe pandemic outbreaks and setting a date by which such plans should be completed.

At this time, all of the organizations subject to the April 2003 "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" are planning for a pandemic, including a severe outbreak, and identifying measures to reduce their vulnerabilities to such events. In addition, all of these organizations have been subject to supervisory review over the past several months, and their contingency plans generally address the four elements recommended in the draft report.

The Agencies have incorporated reviews of organizations' pandemic planning efforts into our ongoing supervision and oversight processes to ensure those organizations are updating their plans as new information becomes available and incorporating lessons learned from market exercises. We follow up to ensure any weaknesses in the ongoing pandemic planning process are appropriately addressed by the organization. In addition, we assure you that we will continue to focus supervisory attention on critical financial

market organizations' efforts to address a pandemic. If we find organizations' efforts lagging, we will consider taking additional actions, including those that you recommend.

Again, we appreciate the opportunity to review and comment on the draft report and to reaffirm our commitment to ensuring the readiness and resiliency of critical financial markets to withstand disruptions. We also appreciate the professionalism with which you responded to the technical comments we provided separately.

Sincerely,

John C. Dugan, Comptroller
Office of the Comptroller of the Currency

Stephen R. Malphrus, Staff Director for Management
Board of Governors of the Federal Reserve System

Erik R. Sirri, Director
Division of Market Regulation
Securities and Exchange Commission

2

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Yvonne D. Jones (202) 512-8678 or jonesy@gao.gov

Staff Acknowledgments

In addition to the individual named above, Cody Goebel, Assistant Director; Edward Alexander; Gwenetta Blackwell Greer; Mark Canter; Lon Chin; West Coile; Caitlin Croake; Kirk Daubenspeck; Kristeen McLain; Angela Pun; Susan Ragland; and Barbara Roesmann made key contributions to this report.

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

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548