United States General Accounting Office

GAO

Testimony

Before the House Committee on Financial Services, Subcommittee on Capital Markets, Insurance, and Government Sponsored Enterprises

For Release on Delivery
Expected at 3:00 p.m., EDT
on Wednesday,
February 12, 2003

POTENTIAL TERRORIST ATTACKS

More Actions Needed to Better Prepare Critical Financial Markets

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

GAO
Accountability * Integrity * Reliability

GAO-03-468T

February 2003

POTENTIAL TERRORIST ATTACKS

More Actions Needed to Better Prepare Critical Financial Markets

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-468T, a testimony before the Subcommittee on Capital Markets, Insurance, and Government Sponsored Enterprises, Financial Services Committee, House of Representatives

Why GAO Did This Study

The September 11, 2001, terrorist attacks exposed the vulnerability of U.S. financial markets to wide-scale disasters. Because the markets are vital to the nation's economy, GAO's testimony discusses (1) how the financial markets were directly affected by the attacks and how market participants and infrastructure providers worked to restore trading; (2) the steps taken by 15 important financial market organizations to address physical security, electronic security, and business continuity planning since the attacks; and (3) the steps the financial regulators have taken to ensure that the markets are better prepared for future disasters.

What GAO Recommends

GAO's report recommends that the SEC Chairman work with industry to

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

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

www.gao.gov/cgi-bin/getrpt?GAO-03-468T.

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

What GAO Found

The September 11, 2001, terrorist attacks severely disrupted U.S. financial markets as the result of the loss of life, damage to buildings, loss of telecommunications and power, and restrictions on access to the affected area. However, financial market participants were able to recover relatively quickly from the terrorist attacks because of market participants' and infrastructure providers' heroic efforts and because the securities exchanges and clearing organizations largely escaped direct damage.

The attacks revealed limitations in the business continuity capabilities of some key financial market participants that would need to be addressed to improve the ability of U.S. markets to withstand such events in the future. GAO's review of 15 stock exchanges, clearing organizations, electronic communication networks, and payments system providers between February and June 2002 showed that all were taking steps to implement physical and electronic security measures and had developed business continuity plans. However, some organizations still had limitations in one or more of these areas that increased the risk that their operations could be disrupted by future disasters.

Although the financial regulators have begun efforts to improve the resiliency of clearance and settlement functions within the financial markets, they have not fully developed goals, strategies, or sound practices to improve the resiliency of trading activities. In addition, the Securities and Exchange Commission's (SEC) technology and operations risk oversight, which is increasingly important, has been hampered by program, staff, and resource issues. GAO's report made recommendations designed to better prepare the markets to deal with future disasters and to enhance SEC's technology and operations risk oversight capabilities.

Source: Associated Press.

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

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to appear before you today to discuss GAO's work on how key financial market participants and the financial regulators are working to improve the resiliency of their operations and the financial markets in the event of future terrorist attacks.

Today, I will present the findings from our report *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, GAO-03-414 (Washington, D.C.: Feb. 12, 2003). Specifically, I will discuss (1) how the September 11, 2001, terrorist attacks affected the financial markets and the actions market participants and infrastructure providers took to restore trading; (2) the steps taken by 15 stock exchanges, electronic communication networks (ECN), clearing organizations, and payment systems providers to address physical and electronic security and business continuity planning since the attacks; and (3) the steps financial regulators have taken to ensure that the markets are better prepared for future disasters.

In summary:

The September 11, 2001, terrorist attacks severely disrupted the U.S. financial markets because of the loss of life, damage to buildings, loss of telecommunications and power, and restrictions that were placed on access to the affected area. However, financial market participants were able to recover relatively quickly from the terrorist attacks, as a result of market participants' and infrastructure providers' heroic efforts and because the securities exchanges and clearing organizations largely escaped direct damage. If certain organizations had sustained serious damage, the markets would probably not have been able to reopen by September 17, 2001. Market participants and regulators have acknowledged that the attacks revealed limitations in their business continuity capabilities and that these limitations would need to be addressed to improve their ability to recover if such events occurred in the future. Our review of 15 stock exchanges, ECNs, clearing organizations, and payments system providers between February and June 2002 showed that all were taking steps to implement physical and electronic security measures and had developed business continuity plans. However, organizations still had limitations in one or more areas that increased the risk of disruptions to their operations if such disasters occurred in the future. Although the financial regulators have begun efforts to improve the resiliency of clearance and settlement functions within the financial markets, they have not fully developed goals, strategies, or sound

practices to similarly improve the resiliency of trading functions. In addition, the effectiveness of the Securities and Exchange Commission's (SEC) technology and operations risk oversight efforts—which clearly have increased in importance—have been limited by program, staff, and resource limitations. Some of these issues were also highlighted in a January 2003 report issued by the SEC Inspector General. Our report made recommendations designed to better prepare the markets to deal with future disasters and to enhance SEC's technology and operations risk oversight capabilities. SEC agreed with the thrust of our recommendations.

Market Participants and Infrastructure Providers Employed Innovative Solutions to Restore Trading

The September 11, 2001, terrorist attacks had a devastating effect on the U.S. financial markets with significant loss of life, extensive physical damage, and considerable disruption to the financial district in New York. Damage from the collapse of the World Trade Center buildings caused dust and debris to blanket a wide area of lower Manhattan, led to severe access restrictions to portions of lower Manhattan for days, and destroyed substantial portions of the telecommunications and power infrastructure that served the area. Telecommunications service in lower Manhattan was lost for many customers when debris from the collapse of one the World Trade Center buildings struck a major Verizon central switching office that served approximately 34,000 business and residences. The human impact was especially devastating because about 70 percent of the civilians killed in the attacks worked in the financial services industry, and physical access to the area was severely curtailed through September 13, 2001. Although most stock exchanges and clearing organizations escaped direct damage, the facilities and personnel of several key broker-dealers and other market participants were destroyed or displaced. Market participants and regulators acknowledged that the reopening of the stock and options markets could have been further delayed if any of the exchanges or clearing organizations had sustained serious damage.

The stock and options exchanges remained closed as firms, that were displaced by the attacks attempted to reconstruct their operations and reestablish telecommunications with their key customers and other market participants. In the face of enormous obstacles, market participants, infrastructure providers, and the regulators made heroic efforts to restore operations in the markets. Broker-dealers that had their operations disrupted or displaced either relocated their operations to backup facilities or other alternative facilities. These facilities had to be outfitted to accommodate normal trading operations and to have sufficient telecommunications to connect with key customers, clearing and

settlement organizations, and the exchanges and market centers. Some firms did not have existing backup facilities for their trading operations and had to create these facilities in the days following the crisis. For example, one broker-dealer leased a Manhattan hotel to reconstruct its operations. Firms were not only challenged with reconstructing connections to their key counterparties but, in some cases, they also had the additional challenge of connecting with the backup sites of counterparties that were also displaced by the attacks. The infrastructure providers also engaged in extraordinary efforts to restore operations. For example, telecommunications providers ran cables above ground rather than underground to speed up the restoration of service.

By Friday September 14, 2001, exchange officials had concluded that only 60 percent of normal market trading liquidity had been restored and that it would not be prudent to trade in such an environment. In addition, because so many telecommunications circuits had been reestablished, market participants believed that it would be beneficial to test these telecommunications circuits prior to reopening the markets. Officials were concerned that without such testing, the markets could have experienced operational problems and possibly have to close again, which would have further shaken investor confidence. The stock and options markets reopened successfully on Monday, September 17, 2001 and achieved record trading volumes. Although the government securities markets reopened within 2 days, activity within those markets was severely curtailed, as there were serious clearance and settlement difficulties resulting from disruptions at some of the key participants and at one of the two banks that clear and settle government securities. Some banks had important operations in the vicinity of the attacks, but the impact of the attacks on the banking and payment systems was much less severe.

Regulators also played a key role in restoring market operations. For example, the Federal Reserve provided over $323 billion in funding to banks between September 11 and September 14, 2001, to prevent organizations from defaulting on their obligations and creating a widespread solvency crisis. SEC also granted regulatory relief to market participants by extending reporting deadlines and relaxed the rules that restrict corporations from repurchasing their shares. The Department of the Treasury also helped to address settlement difficulties in the government securities markets by conducting a special issuance of 10-year Treasury notes.

Attacks Revealed Limitations in Market Participants' Preparedness for Wide-scale Disasters, and Some Limitations Remain

Although financial market participants, regulators, and infrastructure providers made heroic efforts to restore the functioning of the markets as quickly as they did, the attacks and our review of 15 key financial market organizations—including 7 critical ones—revealed that financial market participants needed to improve their business continuity planning capabilities and take other actions to better prepare themselves for potential disasters. At the time of the attacks, some market participants lacked backup facilities for key aspects of their operations such as trading, while others had backup facilities that were too close to their primary facilities and were thus either inaccessible or also affected by the infrastructure problems in the lower Manhattan area. Some organizations had backup sites that were too small or lacked critical equipment and software. In the midst of the crisis, some organizations also discovered that the arrangements they had made for backup telecommunications service were inadequate. In some cases, firms found that telecommunication lines that they had acquired from different providers had been routed through the same paths or switches and were similarly disabled by the attacks.

The 15 stock exchanges, ECNs, clearing organizations, and payment systems we reviewed had implemented various physical and information security measures and business continuity capabilities both before and since the attacks. At the time of our work—February to June 2002—these organizations had taken such steps as installing physical barriers around their facilities to mitigate effects of physical attacks from vehicle-borne explosives and using passwords and firewalls to restrict access to their networks and prevent disruptions from electronic attacks. In addition, all 15 of the organizations had developed business continuity plans that had procedures for restoring operations following a disaster; and some organizations had established backup facilities that were located hundreds of miles from their primary operations.

Although these organizations have taken steps to reduce the likelihood that their operations would be disrupted by physical or electronic attacks and had also developed plans to recover from such events, we found that some organizations continued to have some limitations that would increase the risk of their operations being impaired by future disasters. This issue is particularly challenging for both market participants and regulators, because addressing security concerns and business continuity capabilities require organizations to assess their overall risk profile and make business decisions based on the trade-offs they are willing to make in conducting their operations. For example, one organization may prefer to invest in excellent physical security, while another may choose to

investment less in physical security and more in developing resilient business continuity plans and capabilities.

Our review indicated that most of the 15 organizations faced greater risk of operational disruptions because their business continuity plans did not adequately address how they would recover if large portions of their critical staff were incapacitated. Most of the 15 organizations were also at a greater risk of operations disruption from wide-scale disasters, either because they lacked backup facilities or because these facilities were located within a few miles of their primary sites. Few of the organizations had tested their physical security measures, and only about half were testing their information security measures and business continuity plans.

Regulators Have Addressed Operations Risks but Have Not Developed Complete Strategies and Practices to Better Assure Recovery of Trading

Securities and banking regulators have made efforts to examine operations risk measures in place at the financial market participants they oversee. SEC has conducted reviews of exchanges, clearing organizations, and ECNs that have generally addressed aspects of these organizations' physical and information security and business continuity capabilities. However, reviews by SEC and the exchanges at broker-dealers generally did not address these areas, although SEC staff said that such risks would be the subject of future reviews.[1] Banking regulators also reported that they review such issues in the examinations they conduct at banks.

Regulators also have begun efforts to improve the resiliency of clearing and settlement functions for the financial markets. In August 2002, the Federal Reserve, Office of the Comptroller of the Currency, and SEC jointly issued a paper entitled the Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.[2] This paper sought industry comment on sound business practices to better ensure that clearance and settlement organizations would be able to

[1]In addition to SEC's oversight, stock and options exchanges act as self-regulatory organizations that oversee their members' activities.

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

resume operations promptly after a wide-scale regional disaster.[3] The regulators indicated that the sound practices would apply to a limited number of organizations that perform important clearing functions, as well as to between 15 and 20 banks and broker-dealers that also perform clearing functions with sizeable market volumes.

The regulators that developed the white paper appropriately focused on clearing functions to help ensure that settlement failures do not lead to a broader financial crisis. However, the paper did not similarly address restoring critical trading activities in the various financial markets. The regulators that developed the paper believed that clearing functions were mostly concentrated in single entities for most markets or in a very few entities for others and thus posed a greater potential for disruption. In theory, multiple stock exchanges and other organizations that conduct trading activities could substitute for each other in the event of a crisis.

Nevertheless, trading on the markets for corporate securities, government securities, and money market instruments is also vitally important to the economy; and the United States deserves similar assurance that trading activities also would be able to resume when appropriate—smoothly and without excessive delay. The U.S. economy has demonstrated that it can withstand short periods during which markets are not trading. After some events occur, having markets closed for some limited time could be appropriate to allow emergency and medical relief activities, permit operations to recover, and reduce market overreaction. However, long delays in reopening the markets could be harmful to the economy. Without trading, investors lack the ability to accurately value their securities and cannot adjust their holdings.

The September 11, attacks demonstrated that the ability of markets to recover could depend on the extent to which market participants have made sound investments in business continuity capabilities. Without clearly identifying strategies for recovery, determining the sound practices needed to implement these strategies, and identifying the organizations that could conduct trading under these strategies, the risk that markets may not be able to resume trading in a fair and orderly fashion and without excessive delays is increased. Goals and strategies for resuming

[3]A wide-scale disruption is defined as one that causes severe disruptions of transportation, telecommunications, power, or other critical infrastructure components in a metropolitan or other geographic area and in adjacent communities economically integrated with the area.

trading activities could be based on likely disaster scenarios and could identify the organizations that are able to conduct trading in the event that other organizations could not recover within a reasonable time. Goals and strategies, along with guidance on business continuity planning practices, and more effective oversight would (1) provide market participants with the information they need to make better decisions about improving their operations, (2) help regulators develop sound criteria for oversight, and (3) assure investors that trading on U.S. markets could resume smoothly and in a timely manner.

SEC has begun developing a strategy for resuming stock trading for some exchanges, but the plan is not yet complete. For example, SEC has asked the New York Stock Exchange (NYSE) and NASDAQ to take steps to ensure that their information systems can conduct transactions in the securities that the other organizations normally trade. However, under this strategy NYSE does not plan to trade all NASDAQ securities, and neither exchange has fully tested its own or its members' abilities to trade the other exchanges' securities.

SEC's Automation Review Policy Program Could Be Strengthened

Given the increased threats demonstrated by the September 11 attacks and the need to assure that key financial market organizations are following sound practices, securities and banking regulators' oversight programs are important mechanisms to assure that U.S. financial markets are resilient. SEC oversees the key clearing organizations and exchanges through its Automation Review Policy (ARP) program. The ARP program—which also may be used to oversee adherence to the white paper's sound practices—currently faces several limitations. SEC did not implement this ARP program by rule but instead expected exchanges and clearing organizations to comply with various information technology and operations practices voluntarily. However, under a voluntary program, SEC lacks leverage to assure that market participants implement important recommended improvements. While the program has prompted numerous improvements in market participants' operations, we have previously reported that some organizations did not establish backup facilities or improve their systems' capacity when the SEC ARP staff had identified these weaknesses. Moreover, ARP staff continue to find significant operational weaknesses at the organizations they oversee.

An ARP program that draws its authority from an issued rule could provide SEC additional assurance that exchanges and clearing organizations adhere to important ARP recommendations and any new guidance developed jointly with other regulators. To preserve the

flexibility that SEC staff considers a strength of the current ARP program, the rule would not have to mandate specific actions but could instead require that the exchanges and clearing organizations engage in activities consistent with the ARP policy statements. This would provide SEC staff with the ability to adjust their expectations for the organizations subject to ARP, as technology and industry best practices evolve, and provide clear regulatory authority to require actions as necessary. SEC already requires ECNs to comply with ARP guidance; and extending the rule to the exchanges and clearing organizations would place them on similar legal footing. In an SEC report issued in January 2003, the Inspector General noted our concern over the voluntary nature of the program.[4]

Limited resources and challenges in retaining experienced ARP staff also have affected SEC's ability to more effectively oversee an increasing number of organizations and more technically complex market operations. ARP staff must oversee various industrywide initiatives, such as Year 2000 or decimals pricing, and has also expanded to cover 32 organizations with more complex technology and communications networks. However, SEC has problems retaining qualified staff, and market participants have raised concerns about the experience and expertise of ARP staff. The SEC Inspector General also found that ARP staff could benefit from increased training on the operations and systems of the entities overseen by the ARP program. At current staff levels, SEC staff report being able to conduct examinations of only about 7 of the 32 organizations subject to the ARP program each year.[5] In addition, the intervals between examinations were sometimes long. For example, the intervals between the most recent examinations for seven critical organizations averaged 39 months.[6]

Having additional staff, including those with technology backgrounds, could better ensure the effectiveness of the ARP program's oversight. SEC

[4]SEC Office of Inspector General, *Market Contingency Preparedness*, Report No. 359, (Washington, D.C. Jan. 27, 2003).

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

[6]Standards for federal organizations' information systems require security reviews to be performed at least once every 3 years and recommend that reviews of high-risk systems or those undergoing significant systems modifications be done more frequently. See Office of Management and Budget, *Appendix III to OMB Circular A-130: Security of Federal Automated Information Resources.*

could conduct more frequent examinations, as envisioned by federal information technology standards, and more effectively review complex, large-scale technologies at the exchanges, ECNs, and clearing organizations. If the ARP program must also begin reviewing the extent to which broker-dealers important to clearing and trading in U.S. securities markets are adhering to sound business continuity practices, additional experienced staff and resources would likely be necessary to prevent further erosion in the ability of SEC to oversee all the important organizations under its authority. The increased appropriations authorized in the Sarbanes-Oxley Act, if received, would present SEC a clear opportunity to enhance its technology oversight, including the ARP program, without affecting other important initiatives.

Conclusions

Our work at the 15 organizations we reviewed showed that all of these organizations were taking steps to address physical and electronic security at their facilities and information systems and had business continuity plans to address potential disruptions in their operations, although the extent to which these organizations addressed these issues varied. We recognize that, in addressing these issues, organizations may have to make trade-offs based on their overall risk profile and other business factors.

However, we recommend in our report that SEC take a leadership role and work with market participants to develop goals and strategies to ensure that U.S. markets will be able to resume trading activities after future disasters smoothly and in a timely manner as appropriate.[7] Comprehensive and viable resumption strategies would also require SEC and market participants to identify sound business practices for the organizations that might be called upon to conduct trading after a disaster if others were unavailable. Our report also recommends that these strategies be tested. In addition, SEC has an important oversight role in ensuring that market participants implement sound practices and the improvements to the ARP program that our report recommends should also help ensure that SEC's oversight is as effective as possible.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or other members of the Subcommittee may have at this time.

[7] *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, GAO-03-414, (Washington, D.C., Feb. 12, 2003).