

**RECOVERY AND RENEWAL: PROTECTING
THE CAPITAL MARKETS AGAINST
TERRORISM POST 9/11**

HEARING
BEFORE THE
SUBCOMMITTEE ON
CAPITAL MARKETS, INSURANCE, AND
GOVERNMENT SPONSORED ENTERPRISES
OF THE
COMMITTEE ON
FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTH CONGRESS
FIRST SESSION

—————
FEBRUARY 12, 2003
—————

Printed for the use of the Committee on Financial Services

Serial No. 108-2



U.S. GOVERNMENT PRINTING OFFICE

86-850 PDF

WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

MICHAEL G. OXLEY, Ohio, *Chairman*

JAMES A. LEACH, Iowa	BARNEY FRANK, Massachusetts
DOUG BEREUTER, Nebraska	PAUL E. KANJORSKI, Pennsylvania
RICHARD H. BAKER, Louisiana	MAXINE WATERS, California
SPENCER BACHUS, Alabama	CAROLYN B. MALONEY, New York
MICHAEL N. CASTLE, Delaware	LUIS V. GUTIERREZ, Illinois
PETER T. KING, New York	NYDIA M. VELAZQUEZ, New York
EDWARD R. ROYCE, California	MELVIN L. WATT, North Carolina
FRANK D. LUCAS, Oklahoma	GARY L. ACKERMAN, New York
ROBERT W. NEY, Ohio	DARLENE HOOLEY, Oregon
SUE W. KELLY, New York, <i>Vice Chairman</i>	JULIA CARSON, Indiana
RON PAUL, Texas	BRAD SHERMAN, California
PAUL E. GILLMOR, Ohio	GREGORY W. MEEKS, New York
JIM RYUN, Kansas	BARBARA LEE, California
STEVEN C. LATOURETTE, Ohio	JAY INSLEE, Washington
DONALD A. MANZULLO, Illinois	DENNIS MOORE, Kansas
WALTER B. JONES, Jr., North Carolina	CHARLES A. GONZALEZ, Texas
DOUG OSE, California	MICHAEL E. CAPUANO, Massachusetts
JUDY BIGGERT, Illinois	HAROLD E. FORD, JR., Tennessee
MARK GREEN, Wisconsin	RUBEN HINOJOSA, Texas
PATRICK J. TOOMEY, Pennsylvania	KEN LUCAS, Kentucky
CHRISTOPHER SHAYS, Connecticut	JOSEPH CROWLEY, New York
JOHN B. SHADEGG, Arizona	WM. LACY CLAY, Missouri
VITO FOSELLA, New York	STEVE ISRAEL, New York
GARY G. MILLER, California	MIKE ROSS, Arkansas
MELISSA A. HART, Pennsylvania	CAROLYN MCCARTHY, New York
SHELLEY MOORE CAPITO, West Virginia	JOE BACA, California
PATRICK J. TIBERI, Ohio	JIM MATHESON, Utah
MARK R. KENNEDY, Minnesota	STEPHEN F. LYNCH, Massachusetts
TOM FEENEY, Florida	BRAD MILLER, North Carolina
JEB HENSARLING, Texas	RAHM EMANUEL, Illinois
SCOTT GARRETT, New Jersey	DAVID SCOTT, Georgia
TIM MURPHY, Pennsylvania	ARTUR DAVIS, Alabama
GINNY BROWN-WAITE, Florida	
J. GRESHAM BARRETT, South Carolina	BERNARD SANDERS, Vermont
KATHERINE HARRIS, Florida	
RICK RENZI, Arizona	

Robert U. Foster, III, Staff Director

SUBCOMMITTEE ON CAPITAL MARKETS, INSURANCE, AND
GOVERNMENT SPONSORED ENTERPRISES

RICHARD H. BAKER, Louisiana, *Chairman*

DOUG OSE, California, <i>Vice Chairman</i>	PAUL E. KANJORSKI, Pennsylvania
CHRISTOPHER SHAYS, Connecticut	GARY L. ACKERMAN, New York
PAUL E. GILLMOR, Ohio	DARLENE HOOLEY, Oregon
SPENCER BACHUS, Alabama	BRAD SHERMAN, California
MICHAEL N. CASTLE, Delaware	GREGORY W. MEEKS, New York
PETER T. KING, New York	JAY INSLEE, Washington
FRANK D. LUCAS, Oklahoma	DENNIS MOORE, Kansas
EDWARD R. ROYCE, California	CHARLES A. GONZALEZ, Texas
DONALD A. MANZULLO, Illinois	MICHAEL E. CAPUANO, Massachusetts
SUE W. KELLY, New York	HAROLD E. FORD, Jr., Tennessee
ROBERT W. NEY, Ohio	RUBÉN HINOJOSA, Texas
JOHN B. SHADEGG, Arizona	KEN LUCAS, Kentucky
JIM RYUN, Kansas	JOSEPH CROWLEY, New York
VITO FOSSELLA, New York	STEVE ISRAEL, New York
JUDY BIGGERT, Illinois	MIKE ROSS, Arkansas
MARK GREEN, Wisconsin	WM. LACY CLAY, Missouri
GARY G. MILLER, California	CAROLYN McCARTHY, New York
PATRICK J. TOOMEY, Pennsylvania	JOE BACA, California
SHELLEY MOORE CAPITO, West Virginia	JIM MATHESON, Utah
MELISSA A. HART, Pennsylvania	STEPHEN F. LYNCH, Massachusetts
MARK R. KENNEDY, Minnesota	BRAD MILLER, North Carolina
PATRICK J. TIBERI, Ohio	RAHM EMANUEL, Illinois
GINNY BROWN-WAITE, Florida	DAVID SCOTT, Georgia
KATHERINE HARRIS, Florida	
RICK RENZI, Arizona	

CONTENTS

	Page
Hearing held on:	
February 12, 2003	1
Appendix:	
February 12, 2003	33

WITNESSES

WEDNESDAY, FEBRUARY 12, 2003

Britz, Robert G., President and Co-Chief Operating Officer, New York Stock Exchange	24
Colby, Robert L. D., Deputy Director, Division of Market Regulation, Securities and Exchange Commission	4
D'Agostino, Davi M., Director, Financial Markets and Community Investment, U.S. General Accounting Office	2
Green, Micah S., President, The Bond Market Association	28
Ketchum, Richard, President, NASDAQ Stock Market	22
Kittell, Donald D., Executive Vice President, Securities Industry Association ..	26

APPENDIX

Prepared statements:	
Clay, Hon. Wm. Lacy	34
Israel, Hon. Steve	35
Kanjorski, Hon. Paul E.	36
Maloney, Hon. Carolyn B.	38
Royce, Hon. Ed	39
Britz, Robert G.	40
Colby, Robert L. D.	48
D'Agostino, Davi M. (with attachments)	56
Green, Micah S.	185
Ketchum, Richard G.	278
Kittell, Donald D.	290

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

NYSE response to questions posed by Hon. Richard Baker	298
--	-----

**RECOVERY AND RENEWAL: PROTECTING
THE CAPITAL MARKETS AGAINST
TERRORISM POST-9/11**

Wednesday, February 12, 2003

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CAPITAL MARKETS, INSURANCE
AND GOVERNMENT SPONSORED ENTERPRISES,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to call, at 3 p.m., in Room 2128, Rayburn House Office Building, Hon. Richard H. Baker [chairman of the subcommittee] presiding.

Present: Representatives Baker, Ose, Manzullo, Hart, Brown-Waite, Harris, Renzi, Kanjorski, Sherman, Inslee, Moore, Israel, Capuano, Lucas of Kentucky, Clay, McCarthy, Matheson, Miller of North Carolina, Emanuel, Scott, and Maloney.

Chairman BAKER. I would like to call this meeting of the Capital Markets Subcommittee to order. It is my understanding that Mr. Kanjorski is on his way and will join us momentarily. I would first like to say—as I speak, here comes Mr. Kanjorski.

This is our first meeting of the new session, and we will have a very busy agenda over the coming weeks and months. March and April are particularly going to be time-consuming for Members. But I think we have a lot of important work to do. Today is certainly exemplary of the types of issues with which the committee will be engaged.

We will be in receipt today of a report from the General Accounting Office relative to their assessments of market participants' capabilities to help preclude or, in the adverse consequence, respond to another economic terrorist assault on American soil. And from the initial reading of the report and comments of those who will participate today, although all answers have not been found, it does appear that successful improvements have been in the making. And we look forward to having the committee's assistance in helping the regulators and market participants achieve the level of security needed to ensure that no one can bring our economic system to its knees, an extraordinarily important matter, and I am certain that the committee will return to it on many occasions as circumstances require.

But I extend my welcome to the Members and certainly to the Ranking Member Mr. Kanjorski, I look forward to working with you again this session. And the gentleman is recognized for any opening statement he might make.

Mr. KANJORSKI. Thank you, Mr. Chairman. I think I will move that my full remarks be made part of the record.

Mr. Chairman, first of all, I prize the relationship for the last 8 years that you and I have had as chairman and Ranking Member of this subcommittee, and really take great pleasure in the fact that we were able to rise to the occasion in providing terrorism re-insurance and restoring investor confidence in corporate America to some degree in the last Congress.

Today we are here to examine the physical problems that may exist in a future terrorist attack on the United States and what actions and efforts we should take and what legislation will be necessary to accomplish that end. Also, as I suggested in my amendment to our policy consideration of the committee, we not only should take into consideration the physical effects of a terrorist attack on our economy and our markets, but also what economic disasters could befall the United States, and to start looking at some of the necessary actions to prevent that or to provide the legal authority for appropriate action. And some of the witnesses that are here today representing the various and sundry areas would be instrumental in examining that, because, in my estimation, I believe that terrorism can cause unreasonable and untold loss of life in America, it can cause tremendous physical damage in America, but cannot threaten the national security of America. On the other hand, economic destruction or events could bring down the American economy and, in fact, America in its entirety.

So I think that not only do we have the opportunity to look at the physical effects on the markets and what we can do to shore them up, but also anticipating what economic occurrences may occur over the next several years that could really threaten the economy of the United States. And I look forward to working very closely with you in that end, and I move that my remarks be made part of the record.

[The prepared statement of Hon. Paul E. Kanjorski can be found on page 36 in the appendix.]

Chairman BAKER. Without objection, in their entirety.

Does any other Member wish to make any opening statement at this time? If not, then I would proceed to our first panel of witnesses, and welcome Ms. Davi D'Agostino, who is the Director of the Financial Markets and Community investment Division of the U.S. General Accounting Office.

I think all Members have been provided a copy of your report. Please feel free to summarize and give us any perspectives you think would be helpful to the committee. Welcome.

STATEMENT OF DAVI M. D'AGOSTINO, DIRECTOR, FINANCIAL MARKETS AND COMMUNITY INVESTMENT, U.S. GENERAL ACCOUNTING OFFICE

Ms. D'AGOSTINO. Thank you very much, Mr. Chairman. With your permission, I would like to submit my full written statement for the record, and I would summarize my remarks orally.

Chairman BAKER. Without objection. And all witnesses' testimony will be made part of the official record. Thank you.

Ms. D'AGOSTINO. Thank you very much.

Mr. Chairman, members of the subcommittee, I am pleased to be here today before you to discuss GAO's work on the readiness of the U.S. Financial markets to respond to potential terrorist attacks. The markets are vitally important to our Nation's financial system and to our economy. The devastating attacks on the World Trade Center on September 11th revealed that our markets could be vulnerable to such events.

Today I will talk about, one, how the markets recovered from these attacks; two, the limitations that existed in participants' readiness to recover; and, three, steps that regulators have taken to assure that U.S. markets are better prepared for such attacks and what more needs to be done.

First, because the attacks occurred in the heart of Wall Street, over 70 percent of the nearly 2,800 people who lost their lives worked at financial firms such as broker/dealers and banks. The attacks damaged or destroyed over 400 buildings, and electricity and telephone services were also severely disrupted. Facing enormous obstacles, the utilities, exchanges, and firms worked around the clock and used creative solutions to reopen the markets within days of the attacks. Our report has numerous examples of the amazing efforts behind the market restoration. Still, by that Friday, September 14th, broker/dealers that normally provide 40 percent of market liquidity were not fully ready to trade, and the industry and regulators chose to test the newly established telecommunications over the weekend. On September 17th, the markets reopened, trading record volumes. In retrospect, the markets probably would not have been able to open so quickly if certain organizations had been directly hit.

Second, the attacks also revealed limitations in the disaster planning of many market participants. In some cases firms did not have backup facilities, and others had located their backups too close to their primary sites. Some firms also found that the backup telephone lines they bought from different providers were routed down the same pipes or through the same switches as their primary lines. Our reviews of 15 important exchanges, clearing organizations, ECNs, and payment system processors from February through June 2002 showed that they had taken many steps to prevent disruptions to their operations from physical or electronic attacks. Most had also invested in backup facilities or other measures to be able to recover from such attacks, but many of these 15 organizations still faced increased risk to their operations.

For example, most organizations did not have complete plans to continue operations if the staff at their primary sites were incapacitated. Some of these organizations also faced increased risk of disruption from widescale disasters because their backup facilities were nearby.

Third, the financial regulators have taken some important steps to improve the resiliency of the financial markets to recover from future disasters, but these efforts are not complete. Banking and securities regulators issued a white paper that proposed recovery practices for crucial clearing and settling functions, but they have not made a similar proposal for trading activities. To better assure that trading can also recover in a smooth and timely manner following a disaster, we recommended that SEC take a leadership

role and work with the industry to develop goals and strategies to resume trading. Such strategies could be based on likely disaster scenarios and should identify the organizations that are able to trade in the event that others cannot. SEC also needs to work with the industry to identify sound recovery practices for organizations to adopt—to better assure they can trade after another disaster.

There will be a need to balance the business decisions and risk management trade-offs that individual market participants make with the need for a sound, viable plan for assuring the U.S. markets can resume important trading activities when appropriate. The 9/11 attacks showed that the market's ability to reopen depends on the readiness of key broker/dealers. The plans SEC develops will have to assure that sufficient firms are available to trade, and that customers' accounts at firms unable to operate can be transferred to others who can.

We also recommended that SEC improve its program to oversee operations risks at exchanges, clearing organizations, and ECNs. These improvements included making its voluntary program rule-based, and using a portion of any future budget increases to expand and retain its experienced staff and technical resources.

Mr. Chairman, this concludes my prepared remarks, and I would be happy to answer questions at any time.

Chairman BAKER. Thank you very much.

[The prepared statement of Davi M. D'Agostino can be found on page 56 in the appendix.]

Chairman BAKER. Our next witness is Mr. Robert Colby, Deputy Director, Division of Market Regulation, from the Securities and Exchange Commission. Welcome, Mr. Colby.

STATEMENT OF ROBERT L.D. COLBY, DEPUTY DIRECTOR, DIVISION OF MARKET REGULATION, SECURITIES AND EXCHANGE COMMISSION

Mr. COLBY. Thank you. Chairman Baker, Ranking Member Kanjorski, and members of the subcommittee, I appreciate the opportunity to testify before you today regarding the efforts since the September 11th terrorist attacks to better protect U.S. financial markets and institutions, and to address issues raised in the report released today by the General Accounting Office.

As the GAO recognizes in its reports, participants in the United States financial markets made heroic efforts to recover from the devastation of the September 11th attacks, with the result that all markets reopened successfully within a week after those tragic events. Nevertheless, the Commission and other regulators in the industry have engaged in wide-ranging and intensive efforts to consider the lessons learned from the events of September 11th and strengthen the resiliency of the financial sector so that we are better prepared going forward.

Immediately after the September 11th attacks, the securities industry recognized the need to develop more rigorous business continuity plans that addressed problems of wider geographic scope and longer duration. Market participants have taken a number of significant steps to improve their resiliency, including establishing more robust and geographically disbursed backup facilities for op-

erations in data recovery, improving crisis management procedures, and seeking telecommunications diversity.

The Commission and other financial regulators have also been devoting substantial resources to projects designed to strengthen the resilience of the financial sector. For example, the Commission, working with the Federal Reserve Board and the Office of the Comptroller of the Currency, are in an effort to identify sound practices for business continuity planning for key market participants.

This past August we published for comment a draft white paper that focused on a small but critical group of participants in the U.S. clearance and settlement system. The goal of this project is to minimize the immediate systemic effects of a widescale disruption by assuring that the key payment settlement systems can resume operation promptly following a widescale disaster, and major participants in those systems can recover sufficiently to complete pending transactions. The agencies expect to issue the final white paper next month after an additional amount of consultation with the industry, and then incorporate the sound practices into their respective forms of supervisory guidance.

In addition, Commission staff has been reviewing on an ongoing basis the efforts of the organized markets to strengthen their resiliency in the post-September 11th environment. These markets have taken a variety of steps to improve their physical security, information system protections and business continuity capabilities, and Commission staff continue to work with them to further increase the robustness of their individual plans. In addition, we have been exploring with the markets the possibility of mutual backup arrangements.

As to the resilience of securities firms, the New York Stock Exchange and the NASD have proposed rules that would require all broker/dealers to have business continuity plans that address a number of important areas. We have also been working with the relevant industry associations, the SIA and the Bond Market Association, on their members' business continuity disaster recovery efforts.

To date, the Commission's intensive efforts have focused on measuring and ensuring the resilience of the U.S. clearance and settlement system because, in our view, that infrastructure is the single most important element of the securities markets. As a practical matter, securities transactions cannot be completed in the absence of a functioning clearance and settlement system. Accordingly, the Commission has given priority to initiatives that assure the prompt implementation of vigorous business continuity plans by critical participants in the clearance and settlement system.

The GAO report recommends that the Commission do more to assure the resumption of trading by securities markets and broker/dealers following a major disaster. We share the GAO's views regarding the importance of emergency preparedness of the financial markets, and generally agree with the report's principle: that the financial market should be prepared to resume trading in a timely, fair, and orderly fashion following a catastrophe. But we believe that different, in some cases more complex, policy considerations apply to the resumption of trading than to the resumption of clear-

ance and settlement activities. Because trading activities is relatively fungible across markets and market participants, we are of the view that individual markets and securities firms are less critical to the securities markets than the key clearance and settlement utilities. Were any single securities market to become incapacitated, for example, we believe that trading could be shifted to one or more of the remaining markets. We recognize that sufficient advanced preparation is required for such an arrangement to work smoothly and promptly, and, as I indicated earlier, Commission staff is in the midst of just such an effort.

As to the resumption of trading by securities firms, in our view, strong business incentives exist for broker/dealers to develop robust business continuity plans for their trading operations. Trading operations, of course, are in—at least in good markets, are a source of significant revenue for securities firms, and few would risk a situation where their competitors are in a position to trade and they are not.

I also note that as a provision of liquidity to the market by securities firm is voluntary; they cannot be compelled to resume trading activities.

Finally, there are critical policy considerations relating to the reopening of trading markets following a major disaster that could suggest not compelling the speediest reopening. Difficult judgments may be required to strike the appropriate balance between the desire to resume trading as soon as possible and the practical necessity of waiting long enough to minimize the risks that, when trading resumes, it will be of inferior quality or interrupted by further problems.

For example, in the aftermath of the September 11th events, many praised the decision to wait until Monday, September 17th, to reopen the equity markets as it allowed market participants the preceding weekend to test connectivity in systems and thereby better assure the smooth resumption of trading.

Despite these policy concerns, we nevertheless agree with the GAO that more needs to be done to prepare the securities markets for the resumption of trading in the event of a crisis. Specifically, the Commission intends to consider whether it should identify a time frame against which markets should plan to resume trading following a widescale regional disaster. We also will continue to work with the New York Stock Exchange, NASDAQ, and other organized securities markets to develop and test mutual backup arrangements for various scenarios, and we will pursue efforts to increase the resilience of important shared information systems such as the consolidated market data stream generated for equity and options markets. Any timing goal established for the resumption of trading markets could serve as a useful resumption benchmark for securities firms as well.

In addition, the Commission will consider developing standards in conjunction with the self-regulatory organizations to help assure that broker/dealers are able to provide customers prompt access to their funds and securities even in the face of widescale regional disturbance.

The GAO report also recommends that the Commission improve its oversight of operations risk by issuing a rule to require ex-

changes and clearing organizations to engage in practices consistent with the Commission's automation review policy, or ARP program, and by expanding the resources dedicated to that program. The Commission recognizes the critical role that technology plays in the securities industry and specifically the importance of having in place adequate safeguards and controls over information resources to ensure reliable and timely trading services to investors.

The events of September 11th underscored the financial markets' critical and increasing dependence on the integrity of their systems' infrastructure. In light of the GAO's recommendations, we will consider alternative mechanisms to improve the effectiveness of the Commission's automation oversight, including the appropriateness of rulemaking. We will also assess the additional resources that may be necessary to accomplish the objectives of the ARP program and the GAO report.

Thank you for the opportunity to testify, and I would be happy to answer any questions.

Chairman BAKER. Thank you, Mr. Colby.

[The prepared statement of Robert L.D. Colby can be found on page 48 in the appendix.]

Chairman BAKER. Ms. D'Agostino, it appears from the basic recommendations, there were principally two things I found of interest. One was the resource limitation on ARP staffing and their ability to only review perhaps 7 of 32 particular agencies on an annual basis, which means 4-1/2 years before you would make the full cycle. So resource allocation for the technical folks we need to make that system work is essential.

But number two, and I think Mr. Colby's closing comments spoke to it briefly, is the advisability of having rulemaking as opposed to voluntary participation as a result of the ARP program findings.

It would appear to me that most of what I have read from the industry perspective is that we should be careful not to mandate something, a particular standard or a particular time line or particular steps to be taken, because each shop is different, each conducts its business in a slightly different manner. But would it not be consistent with the report that we at least by rule adopt goals; that first, after whatever event may occur—and that obviously is the difficult thing to predict—that efforts should be made for an immediate operability, but subject to some period of time to test? I think the lessons of September 11 was the Monday, September 17th success. Had it opened and stumbled, I think the repercussions would have been significant. Can't we get to a—could we not construct a goal, an operational plan that would not so constrain individual companies or participant, but yet set a standard in place that would be mandatory?

Ms. D'AGOSTINO. Actually the ARP program and the ARP policy is sort of like a goal. It does not have very specific technical standards to which an organization must live up, and it is not with a huge amount of specificity that programs are reviewed. It is more of a performance-based-type policy and program that they operate with now, and that would be consistent with what we are recommending.

We acknowledge, I think, in our conclusions in our report the need for flexibility and for technology to continue to evolve and to have the opportunity to avoid—well, to ensure avoidance of a one-size-fits-all or a cookie cutter approach where everybody has to do the same thing, because of course there are many technology paths just as there are for physical security solutions and other issues.

Chairman BAKER. But you do believe that the ARP findings or recommendations should be in the form of a mandatory requirement as opposed to voluntary participation?

Ms. D'AGOSTINO. Actually they are mandatory on the ECNs now. SEC did pass a rule that makes compliance with the ARP by the ECNs required. So if we made that an across-the-board requirement for all organizations subject to ARP, it would simply even it out.

Chairman BAKER. Right.

Mr. Colby, listening to our exchange, do you have a concern or caution about mandatory ARP compliance or not?

Mr. COLBY. Let me drop back and explain why the ARP program is the way it is. It was developed a number of years ago, and it is a little different for the Commission, because it was a program of looking at the computer resources and the process of examining, assessing, evaluating computer resources is something that has been developing as automation has grown. So we did it on a voluntary basis in part because we didn't want to freeze into place something that was still in an evolving state, and it stayed voluntary because on the whole, given our influence over the self-regulatory organizations that it applies to, it has worked quite effectively.

Now, within the ARP process, it assesses, processes, and controls the system development mechanisms. There is room for differing of opinions. So our people might come in and say, we think that there is this weakness in your process, and the SROs may come back and say, well, we disagree.

I think the sort of rule that the GAO is talking about is one that mandates the process, in compliance with the process, as opposed to any particular result that would come out of that evaluation.

Chairman BAKER. But the compliance for the ECNs which is mandatory was principally centered, as I understand it, on the reality that they were not open outcry systems, they were a communications-based marketplace. And as I view the markets today, we are clearly moving rapidly to emulate that structure. And it would seemed to me that verification by someone that the communication skills and abilities, whatever the platforms may be, can have functionality even after the aftermath of one of these events would be advisable.

Mr. COLBY. We absolutely agree. The ARP rules that applied to ECNs were applied in part because of their structure, but in part because they are not in the same regulatory state as the self-regulatory organizations which we examine, review their rules, and have a lot of interaction. But the ECNs are typically private organizations, for-profit organizations, and so in that sense it seems it needed to be mandatory.

It also is a process-based approach, and so I think what they are recommending could be transferred over to the self-regulatory organizations.

Chairman BAKER. I have exhausted my time, but just one more quick question about the funding levels for the ARP program.

Mr. COLBY. Funding levels.

Chairman BAKER. Yes. Where are we? What has the Congress done in relation to that issue? And where is the agency with regard to requests for this year?

Mr. COLBY. As you know very well, we have had a funding problem over the years, and the ARP program is one of the things that has been constrained by those funds. Another practical problem that constrains that process is—and this committee by moving to address it—that hiring the sort of people that go into the ARP process is quite difficult, partly because the government process for hiring is sort of skilled automation experts that we need is protracted, and partly because with the dot.com boom, these people were just not available.

Chairman BAKER. Well, your ringing endorsement of the Oxley-Baker bill has been duly noted. Thank you.

Mr. COLBY. And that is what I intended.

Chairman BAKER. Thank you very much.

Mr. Kanjorski.

Mr. KANJORSKI. Thank you very much, Mr. Chairman.

Most of your concentration has been on physical damage and a physical terrorist attack and what the implications of that are in the marketplace; is that correct?

Mr. COLBY. Our program both looks at physical and at information vulnerabilities.

Mr. KANJORSKI. But as a result of physical damage.

Mr. COLBY. Not necessarily. It also looks at the security measures that are taken with respect to cyberthreats and the like. Cyberthreats are quite difficult, of course, to predict and respond to, but it does intend to look at that, and it has been a focus of the ARP process.

Mr. KANJORSKI. If the attack on September 11th had, in fact, not taken place against the World Trade Center buildings in New York but in the Sears building in Chicago, has anyone done a study as to what the disruption of the market, if any, and the economic effect of the terrorist attack on the market, if any, would have been relative to what did happen?

Mr. COLBY. There is a very high concentration of critical financial markets in the Chicago area, and it is something that we have been focused on. Our agency, of course, is only the securities markets.

Mr. KANJORSKI. I guess I'm not directing myself, because that again goes to the question of physical damage. I am trying to say, has anybody said what the physical damage in the delay of opening the markets and functioning in a physical way in the market as compared to the economic impact of a terrorist attack was on the economy of the United States? In other words, I would like to know in that September period after—September through October after the attack when we had the tremendous downturn in the market, was that a result of the economy, or was that just a result of fear

in the marketplace and the failure and the time required to open the markets and get back to an orderly operation?

Mr. COLBY. I think it is indisputable that the immediate drop—there was a 3 percent drop on the day after the markets opened, was clearly a result of concern about what the terrorist attack meant. I don't think that the rest of the fall in the markets can be attributed to that directly. We have participated, but not been chiefly responsible, in economic studies done by what is now the Homeland Security Department about the economic consequences of a terrorist attack in trying to assess how the September 11th and how a possible future attack might affect the economy.

Mr. KANJORSKI. And have you participated in those, or should you participate?

Mr. COLBY. We have participated to provide our expertise, to try to give them a sense of what the impact on the markets would be. And then—

Mr. KANJORSKI. If you can answer: The CIA Director today testified that the untested potential exists for an ICBM to—with an atomic warhead to hit the cities on the west coast of the United States. Making the assumption that two 20-kiloton bombs were to hit either San Diego, Los Angeles, San Francisco, Portland, or Seattle, what would be the ramifications to the economy of the United States? And are we looking at that in terms of—are we just being functional and physical here in looking at how to handle the marketplace as opposed to what we have to think about the disruption of the economy?

Mr. COLBY. This level of response is the functional and physical. There are elements of the government that are looking at the broader consequences. It is being conducted in the context of the Homeland Security Department, and there is an entire community of which we are one small member whose title is The Economic Consequences of An Attack, and they are trying to both scope out what those sort of consequences would be and also what sort of steps might be necessary to respond to them.

Mr. KANJORSKI. So this committee should start thinking in terms of not only the physical consequences of terrorism, but the economic consequences of terrorism and other economic circumstances unrelated to terrorism as to what kind of structures and processes should be put in place in an anticipatory way in order to keep the economy sufficiently existing so that we don't really lose the war.

Mr. COLBY. The physical and functional is just the beginning of the process of trying to address what the consequence of a terrorist attack would be.

Chairman BAKER. Thank you, Mr. Kanjorski.

I want to recognize the gentleman from California and welcome him to his new capacity as vice chair of the capital market subcommittee. Mr. Ose.

Mr. OSE. Thank you, Mr. Chairman. Your wish is my command.

Mr. Colby, my questions really relate to the alternative means by which liquidity and transparency can be provided to the marketplace in the event of a catastrophe. If I understand the testimony of yourself and Ms. D'Agostino and the others who are going to follow, there is a certain level of redundancy between, say, New York, the Pacific, and the American and the NASDAQ and some of the

other ECNs to the extent that New York Stock Exchange is prepared to trade the top 250 volumewise companies traded on NASDAQ. And I imagine there are similar relationships elsewhere. It is my—I am aware that the NASDAQ folks have come forward seeking to have—I am trying to remember the language that they used, but to have the SEC designate NASDAQ as an approved marketplace for any number of reasons, one of which might be to facilitate liquidity and transparency in the event of a catastrophe.

Now, I have been working on this for 2 or 3 years. I am still interested in it. I am going to keep sending letters. I would like to know what the status is on the application that was filed in November of 2001 by the advocates for NASDAQ in terms of their application.

Mr. COLBY. NASDAQ's exchange application is still being processed. There were both practical, legal, and policy concerns. The most fundamental policy concern emanated from a concern of what an exchange should be. One of the first things we expect to do with our new chairman when he is confirmed is to move this application forward.

May I drop back and address the first part of your question, which is that we believe—and I hope that NASDAQ will confirm—that from an operational standpoint, that they are just as prepared to address the sort of concerns about redundancy in their current status as they would be as an exchange. And so while there are very good reasons to be forwarding the exchange application, I am hopeful, and I think Rick Ketchum could confirm it, that the question of backing up the New York Stock Exchange and other markets is not one of the things that turns on an exchange application registration.

Mr. OSE. So what are the conditions that have yet to be resolved on this? I mean, 2 or 3 years is a long time.

Mr. COLBY. Two or three years is a long time. This is a monumental enterprise. The rules and rule changes that they submitted would fill half of this table.

Mr. OSE. Do all the rule changes still need to be vetted, or have you narrowed it down to a few?

Mr. COLBY. We have narrowed it down to a few major and a larger number of minor changes, but the minor are more minor. The sort of things that are still at issue besides the question of how much, what the nature of the market has to be, is a question of what is the scope of the registered exchange? What sort of representation must members be provided in the governance of the exchange? Because there is a statutory requirement for fair representation of members, and that has to be reconciled to a corporate, for-profit, ownership structure. Those are the primary issues.

The minor issues involve such things as what sort of short sale rules should apply, whether the exchange requirements about separation of member trading should apply to this sort of an exchange when it applies to all other sorts of exchanges. And there is a list of smaller issues, but those are the key ones.

Mr. OSE. It is my understanding that the governance issue had been resolved. And if I read, I think it was Mr. Ketchum's next testimony, they are, if I read this correctly, prepared to abide by the short sale rules that exist in NYSE today.

So, my time has expired, Mr. Chairman, but I would be following up in writing because I intend to get this thing resolved. No is an answer. But if it is no, let us get to it. All right?

Mr. COLBY. We agree. We hope to be moving it forward.

Mr. OSE. Thank you, Mr. Chairman.

Chairman BAKER. Thank you, Mr. Ose.

Chairman BAKER. Mrs. McCarthy?

Mrs. MCCARTHY. Thank you. This is my first day on this committee, so I don't know whether my questions are going to be that intelligent. But just listening to—well, you both have been talking about, and then obviously with the heightened security on Friday, are we better off today than we were on September 11th? And how are we going to handle it? And just listening to the debate, and I know government runs very slowly, but just God forbid something did happen, and we are still waiting almost a year and three-quarters on waiting for some rules to come through so we can be ready to go the following day, hopefully, if we had an attack. Where are we today if something happened by the end of this weekend?

Mr. COLBY. We are much better off today than we were on September 11th, and I can give you some specific examples of things that have changed. There is still work to be done, and I think what you see is the GAO's pointing out that there is work to be done, but let us not minimize the work that has been done.

All the major markets have dropped back and looked at their resiliency and what they can be doing to continue trading in the case of a problem with their main trading site. The New York Stock Exchange will detail for you their plans for a backup trading site. NASDAQ has long had two separate locations. There are efforts well under way in the clearance and settlement system in order to create more diversity. The main processing sites have been relocated. And there—each of the major securities firms, and I believe it is true for banks, though that is not our responsibility, have been spending the time since September 11th completely revising their business continuity plans to take into account the new realities, and many of them have already put in place more resilient operation centers. There are vastly improved coordination mechanisms between—within the firm. Don Kittell will talk about the SIA's efforts with respect to command centers and business continuity planning.

And so I think—I don't know if you would agree, Davi—that we have come a very long way, but there is room to go farther.

Mrs. MCCARTHY. Because my only concern is, and this will be my final question, that when we had a heightened security on Friday, then the market, I believe, dropped quite a few points on Monday and Tuesday, if I am correct. My concern is obviously the security firms, they can only do as well as the confidence of the people that are buying their stocks. So obviously they are going to do everything possible to make sure that people feel confident. And I haven't seen anything, you know, out there to the general public on talking about how well we have done and how well we came back.

I was down on Wall Street a few days after September 11th, and to me it was amazing how everybody worked together. To me it was amazing how everybody just came together to get this up, be-

cause we certainly—as horrible experience it was, and I lost an awful lot of people from Camp Fitzgerald in my district, but the bottom line is, we can't let the terrorist win, because whether they are going to attack us or not, the majority of people do believe it is going to be New York or D.C. Whether it is true or not, that is what people believe in. And we have to do—I personally think we have to do a better job on just getting it out to the normal consumer that we are ready, and it is not going to affect us the way it did on September 11th.

Thank you for your testimony.

Chairman BAKER. Thank you, Mrs. McCarthy.

I didn't announce earlier, but it is a general understanding that the recognition of Members for questions will proceed based on seniority by time of arrival. So the short message is if you are here on time when the meeting starts, you have got a good chance of getting recognized early.

Mrs. MALONEY. Point of personal privilege?

Chairman BAKER. Certainly.

Mrs. MALONEY. I am not a member of the committee, but may I ask unanimous consent to place into the record a statement? I have a conflict with another meeting, and I wanted to thank my constituents, Rick Ketchum from NASDAQ and Robert Britz from New York Stock Exchange, for appearing today and for all of their work in combating terrorism and getting our financial markets ready.

Chairman BAKER. Without objection, and certainly appreciate their efforts.

Mrs. MALONEY. Thank you, Mr. Chairman, and thank you for having this hearing.

Chairman BAKER. Certainly.

Ms. Hart.

Ms. HART. Thank you, Mr. Chairman. I missed, unfortunately, a big piece of the GAO testimony, so I am going to ask Ms. D'Agostino a question that she may have answered already, so bear with me.

I understand the concern, I was on the committee when we went through September 11th and all the aftermath, the concern that everybody had about everybody being able to get back to work and everything going again. As far as recommendations that the GAO has made, do you rank the actual physical proximity of the alternative place where they would work if they can't be where they are supposed to be of any high importance at all, the physical proximity of sort of the alternative? You mentioned something in the testimony about the—sort of always having an alternative place to be. Is that relevant, or is that something that is important?

Ms. D'AGOSTINO. I think we would say that it is very important to have backup facilities, particularly if you are a critical organization and no alternatives exist for your services and functions. And again, we do not—GAO hasn't developed a position on the right number of miles between a primary and backup facility. I mean, we haven't even considered that. But clearly from our lessons learned from the 9/11 experience, having a backup facility to handle your operations or to take you far enough away from a widescale incident is a good idea. So I think that is about where

we stand on it. But we think it is important to have backup facilities.

Ms. HART. Okay. You are not going to micromanage where and how and all those sorts of things, or you have no suggestions that are really specific in that way?

Ms. D'AGOSTINO. Not about mileage, but about functionality, yes, it is a good idea to have a backup facility that can perform your critical operations in full.

Ms. HART. There was an—I was just reading the testimonies—a mention of 60 percent wasn't enough; 60 percent of your operations wasn't enough.

Ms. D'AGOSTINO. I believe 60 percent of the market liquidity was ready to trade represented by broker/dealers.

Ms. HART. Okay.

Ms. D'AGOSTINO. Forty percent was not ready to trade on Friday, the 14th of September. That 40 percent was not fully ready.

Ms. HART. So would you expect them all to be fully ready? Should they all be able to be fully ready with an alternative facility?

Ms. D'AGOSTINO. I think that is a question for the SEC and the industry to work out in its strategy and plan for restoring market operations or trading operations after a disaster.

Ms. HART. Since the SEC is here, what do you think about that?

Mr. COLBY. Well, I don't think you can plan or try to compel everyone to be able to come back, because you don't know what the consequences could be. And, frankly, we don't need to because we have multiple competing providers of services. There are two positive consequences from that. The first is that many clients can just move. If one broker is not operational, they use another broker. And because of that, the brokers have very strong incentive not to have their customers leave them, so they have strong business incentives that align with the government objectives in order to be able to continue operating. And it is most true with respect to the securities firms. It is also true with respect to securities markets, because there are very few products, publicly-traded products, in this country that are traded only in one location, which gives a built-in resilience to the system.

Ms. HART. Are you hopeful then that as this issue is being—continues to be examined, that most organizations involved will certainly, as a matter of their own survival, make the best plan they possibly can and expend whatever resources they have at their fingertips to be able to do that? It is going to be a huge cost to them.

Mr. COLBY. It will be a huge cost, and I think we have to keep those costs in mind particularly in an environment where there is not just one central utility that is providing the service, but a number of competing entities.

It is said that the shelf life of a securities firm must be measured in weeks. If they are not operational and their competitors are, their business is gone very quickly, and it may never return. And so securities firms have an incentive to operate—which is not to say we don't need to set guidelines and objectives and standards, but I think the incentives are aligned.

Ms. HART. Thank you, Mr. Chairman.

Chairman BAKER. Thank you, Ms. Hart.

Mr. Emanuel?

Mr. EMANUEL. Thank you, Mr. Chairman.

As somebody representing Chicago, and as a former board member of the Chicago Mercantile Exchange, as I listen to your testimony and read the report, more and more what you seem to have talked about was the physical location. And given that more and more trading is going electronic, away from the open outcry—talking about my area—we have the options exchange and the clearinghouse most specifically that has been a concentration. I kind of recognize the problem of dealing with cyberterrorism. But given where the markets are going every day increasingly—I do think you have to worry about physical location, backup facilities, dealing with the clearinghouse—my bigger concern is the electronic piece of this market, where the market really is going tomorrow, and less about the physical locations.

I am not—given that we have the Board of Trade, the options, and the Merc and the stock exchange in Chicago, I do care about the physical locations, but if you just look at the trading future of where they are going, where handhelds are now on the floor, I am more and more interested about the electronic piece of this business and not the physical location of it.

I may have to go into a witness protection plan now that Chicago hears I could care less about the physical. I don't care less about it, but what I care about is what is going on electronically and what you are doing to protect that. And as you said, it is the most difficult part of what we have to do, and yet if you look at where trading is today and how it is moving tomorrow, it is almost purely electronic, and you could do that by each of the exchanges and go through them and talk about what their futures are like. And having sat on the Merc board, that was the preoccupation of the board for a long time, and that is where the exchange is going now.

Mr. COLBY. You are right in pointing out that the physical threats are less significant if you have an electronic market, because as long as you have dispersion between your operating centers, the market can continue. In fact, some of the markets that have physical floors, have as their backup plans an electronic market. So they recognize that, though that is not where they want to go to, but if they have to maintain their operations, they can do it electronically, which then puts a premium on cybersecurity. And this is something that it is very much a focus. It is a focus for the government, from the President's Committee on Infrastructure Protection right on through down to our level. And there have been a lot of measures taken by the various markets and clearance and settlement systems to try to assess and protect their information security.

Mr. EMANUEL. Well, I want to drive this point home, because as I look at this report, obviously you have the shadow of September 11th that hangs on it, but the truth is I don't want to protect for September 11th alone. They are not going to just do a repetition of September 11th. We have to actually prepare for the next attack that is going to be, in my view, a lot different than September 11th. And we have to deal with where our exchanges are going, where our trades are going.

And my one last comment as well as question is given that a lot of these functions today—the clearinghouse in Chicago is really a consolidation for the different exchanges. That consolidation actually makes it at one level economically efficient and another level a far greater target for—and easier to disrupt for a terrorist organization. And I don't even know if that—that is more of a statement than a question. So, given the trends of what is going on in the industry, I want us to be thinking about the future not so much about laying in place the protections about what happened in the past and only the past. Thank you.

Chairman BAKER. Thank you, Mr. Emanuel.

Ms. Brown-Waite.

Ms. BROWN-WAITE. Thank you, Mr. Chairman. I apologize for not being here sooner; I had some constituents from my district.

This question may have already been answered, but have the agencies actually reviewed the inter-agency white paper that set a goal that may be so costly and unreasonable that it would be unachievable? Have you done an economic analysis of what this recommendation would mean to the industry? And I think I would ask this to Mr. Colby.

Mr. COLBY. We have tried to do an economic analysis. We received comments on the one that was initially put out. We are in the process of revising it. We plan a process of consulting with the firms to try to assess what the impact of the revised statement would be in order to try to take into account the cost impacts.

Ms. BROWN-WAITE. But do you actually have an estimate of what the cost impacts are?

Mr. COLBY. We have a sense from the people, the firms that would be affected, of what the costs were. These are, of course, proprietary expenses. We have not made them public, but we have been pursuing with them what the costs would be.

Frankly, a lot of the cost depends on the implementation schedule, because if it is something that can be worked into their computer planning and automation development, it is much less expensive than if it has to be done immediately.

Ms. BROWN-WAITE. Thank you, Mr. Chairman. I yield the rest of my time.

Chairman BAKER. Thank you very much.

Mr. Scott?

Mr. SCOTT. Yes. Thank you, Mr. Chairman.

In the wake of 9/11, of course, we have put together the Department of Homeland Security. I would be interested in knowing both of your opinions.

What do you see the role that the new Homeland Security Department will play in ensuring that we have continuity in the event of another terrorist attack and in preparation, particularly as it relates to business continuity and investor confidence?

Mr. COLBY. The topic of business continuity and investor confidence is one that is important to the homeland security. To date, they have been interacting with the group that was set up before the Homeland Security Department called the Financial and Banking Information Infrastructure Committee, chaired by the Treasury Department, of which we, the bank regulators and a number of other agencies, are part.

They have been working through this group in order to try to coordinate policies and improve the development. But from our interaction with them, it is very clear that this is a matter that is of concern to that Department.

Mr. SCOTT. Are you satisfied with what the Department of Homeland Security is doing or projected to be doing to ensure that our markets will continue to operate? Is there anything else you would recommend?

Mr. COLBY. My sense is that they are taking this very seriously, and it is going to be one of the important items on their agenda.

Mr. SCOTT. Okay. Thank you Mr. Chairman.

Chairman BAKER. Thank you, Mr. Scott.

Ms. Harris.

Ms. HARRIS. Thank you, Mr. Chairman.

With a follow-up to Ms. Brown-Waite's question concerning technology, is there an overall assessment concerning cyberterrorism and how this would affect the financial markets?

And then secondly, how would you characterize the state of preparedness with regard to future terrorist attacks and how they will affect our financial markets?

Mr. COLBY. I did not hear the last question, I'm sorry.

Ms. HARRIS. How would you characterize the state of preparedness of our financial markets with respect to future terrorist attacks?

Mr. COLBY. Cybersecurity is, obviously, more amorphous than physical threats because with physical threats you can assess a particular location or building and say, what happens if that was damaged?

Threats can come in a variety of different shapes and forms, but there are very active efforts on the part of the financial institutions and the self-reporting organizations that are dependent on information—and the securities markets are, at base, an information business—to protect themselves from the threats that could disable their operations or create polluted information flows within the system.

So our sense is—and we are not alone in looking at this, but a number of consultants and advisers have looked at it—it is something that you need to stay focused all the time, but the efforts that have been dedicated to it have been very extensive and effective.

The overall state of preparedness has come a long way. We are in much better shape than we were on September 11, but there is more to be done. I think that both the agencies that are in charge of it, the self-regulatory organizations that operate trading markets and oversee members, and the financial firms themselves, are all very focused on preparedness at the very highest levels of their institutions. It went from being one more cost item to being a critical matter for each of these institutions.

Chairman BAKER. Thank you, Ms. Harris.

Mr. Inslee?

Mr. INSLEE. Thank you.

I wanted to ask about your findings on the automated review group, the ARP. You seemed to suggest that—and I missed your oral testimony, I am just reading here, I am sorry—but you seem

to suggest that there were inadequate resources to really complete some fundamental reviews. I think you noted that there were only 7 out of 32, if I read your testimony right, that have been completed, which to me was a pretty glaring failure given the risk to these markets.

Is that—from your review, is that simply a result of lack of resources and appropriations to the SEC? Is there some other inhibition? What is the reason for that failure?

Ms. D'AGOSTINO. The resources—the automation program could use more resources and more experience levels. The problem is—and this is true pretty much throughout the government, it is not unique to the SEC; even GAO has some challenges in this area of human capital—getting good technical people and being able to pay them enough to retain them.

In saying that, I don't mean to belittle our recommendation. It is not just an SEC problem, but it is an important program, we think, from the standpoint of the markets. It is the only oversight program going that does what it does. It has been particularly challenged in terms of being able to handle high turnover rates, low staffing levels, sometimes as low as three to four people. They are now up to 10, I believe, to handle 32 market organizations.

As I think our report mentioned, Federal standards recommend reviewing high-risk organizations once every year or two. This puts the SEC program in a kind of straits.

Mr. INSLEE. This is one of the reasons we were concerned when the administration tried to cut the SEC budget, at least below what it was promised. We hope at the end of this budget cycle that sanity is restored and we get resources for getting this done. Thank you for letting us know about that.

Ms. D'AGOSTINO. Thank you.

Chairman BAKER. Mr. Renzi?

Mr. RENZI. Thank you, Mr. Chairman.

Thank you, Ms. D'Agostino and Mr. Colby. I appreciate your time and the detail and the professionalism of your report.

I come from the wildlands of Flagstaff, Arizona, and recently I had an opportunity to sit in on a contingency where a regional attack was simulated at the Northern Arizona University dome. We had the firemen and we had the police out there, and we had helicopter crews come in. It was a regional attack.

I learned that the rail runs through Flagstaff and the major highways run through Flagstaff, and a big gas oil line runs through Flagstaff. I also learned that a communications hub is in that area, one that goes all the way to communicate to the east coast.

I said to myself, if we had a regional attack and it knocked out the ability of L.A. to trade in New York, and we set up this bicoastal confrontation between the L.A. investors not being able to invest if the market stayed open—or would it close? What would happen if all of a sudden we had this East-West conflict based upon regional attacks, particularly in the West, if you don't mind?

Ms. D'AGOSTINO. From a telecommunications standpoint?

Mr. RENZI. Telecommunications, and a communications hub.

Ms. D'AGOSTINO. The telecommunications infrastructure network involves more than single paths for communications to go through, and many different options for switching. So it is not clear that—

Mr. RENZI. That one would be knocked out—

Ms. D'AGOSTINO. You would have to really know where everything is.

Mr. RENZI. When you look at the manufacturing industry and you look at upstream suppliers—I am sure you look at upstream suppliers or vendors who provide you with integral portions of what it takes for you to do business—have you looked from a contingency standpoint at all those integral nodes; not only communications, then, since we are able to go on a different path, but all the upstream providers that are integral to your operation from a contingency standpoint, like a manufacturer operation would look upstream?

Ms. D'AGOSTINO. GAO has not done such a review, to my knowledge.

Mr. COLBY. You as the securities markets are supported by a lot of suppliers that provide various services. Some of them are regulated, some are not.

We have been looking at the regulated ones within the limitations of our resources, and we have been talking to the securities firms about themselves checking about the resilience of their providers, their service providers, because they rely on vendors of various types. So since September 11 there has been an extensive amount of back-checking about resilience.

Mr. RENZI. Right. Any great organization has an Achilles' heel. That is what I am going for here. I am just a small businessman from Arizona is all, but my instincts tell me that if we look at the stock market and we look at other avenues to attack the stock markets, which is in the direct crosshairs of the terrorists, that next time they are going to be smart enough to attack somewhere that directly affects the stock market without attacking New York. So in your course of discussions and development on this, I would urge you to maybe take a look upstream. Thank you.

Chairman BAKER. Thank you, sir.

Mr. Israel?

Mr. ISRAEL. Thank you, Mr. Chairman. I apologize for being late. The Committee on Armed Services has a hearing in conflict with this, so I have been shuffling back and forth.

Several weeks ago I visited with a local company in my district called Applied Visions. They are working with the Defense Advanced Research Projects Agency to develop software that would protect financial institutions and others against a cyberattack, and helps people assess the likelihood of a cyberattack.

One of the things that I learned at that meeting was that some financial institutions in the New York area, I believe the New York Stock Exchange and others, have created a kind of voluntary association, a kind of collective self-defense pact against cyberterrorism. They work together to monitor potential attacks, and then they alert each other if they believe an attack is imminent against any of those that are included in that group.

The problem is that if they are aware of a potential attack against a financial institution outside of that group, there is not much that they can do about it. They do not necessarily share that data. So here you have a group that has the potential of protecting a large number of financial institutions against a cyberattack, but

does not have the wherewithal or the ability or willingness to alert the broader community.

I was wondering whether in your research you were aware of that group, and whether you can make specific suggestions on how it can be broadened to provide the greatest extent of protection to the largest number of financial institutions, rather than a select few.

Mr. COLBY. That is not the only group operating, fortunately. There are other channels to get the information out. There are a variety of information dissemination groups, ISACs they are called. There is one in the securities world operated by SIAC.

Also, on the government level there is a process developed through this FBIIC channel so when a regulator learns of something that affects a regulated entity, they communicate it up so that at a much higher level you can look and see, if there is a pattern here. Once the pattern is identified, the threat can be communicated back down to all people that might be potentially threatened.

Mr. ISRAEL. Are they required to communicate that threat?

Mr. COLBY. There is not a specific rule that requires it, but in practice it is expected and it does happen, because there is a inter-connection between the securities firms and their self-regulators; maybe not quite daily, but a very close interaction beyond that; so this sort of communication is expected to be communicated into the channels and made—and it has happened. It has happened where the firm will say, look, we have just had a problem. The regulators then say a firm has just had a problem. We think it is internal, but we then canvass and check and see if anyone else is having the problems in order to identify whether it is a generalized problem or infectious, or an internal glitch.

Mr. ISRAEL. One final question. Do either of you believe that the current systems that are available to assess threat are effective, or do we need to improve the software or improve other systems so that we are better equipped to assess a potential cyberattack against financial institutions?

Ms. D'AGOSTINO. I know there are a number of software options out there. I know some very large multinational corporations have even developed their own threat and risk assessment and risk management software.

The important thing is the inputs into the decision-making models that the software represents. That would involve some good intelligence information about the threats and who is targeting you and what kinds of possible scenarios. It is development of reasonable and, I guess, viable scenarios for you to play out, then, through the software.

So just as important as software solutions are getting that good data and those viable scenarios to input through those models and get you some reasonable outputs to assess then, and to make decisions on your security solutions.

Mr. ISRAEL. Very good. Thank you. I yield back, Mr. Chairman. Chairman BAKER. Thank you, Mr. Israel.

I want to express to each of you and the agencies you represent my appreciation for your appearance and your work.

Mr. MANZULLO. Mr. Chairman.

Chairman BAKER. Sorry. You are recognized. I apologize.

Mr. MANZULLO. Thank you.

Thank you for coming. I am sorry I was not here for the testimony.

Ms. D'Agostino, as I read the testimony, on page 4 it is absolutely startling that companies that are professionals in back-ups and redundancy systems for the purpose of security and storage of equipment in many cases never took the time to track the path or switches, so that a company's main path or switch would also be the same path or switch of the company hired for the redundant system.

That is pretty dumb. I don't understand how a security company could hold itself out as being an expert—and I see some guys back there nodding their heads, "Yes, maybe we got ripped off." ask for your money back.

But even under a situation where there had been, for example, a fire in the building and not an act of terrorism, this statement is absolutely startling. I am not one big into licensing for professionals, but in your investigation, the people that install these redundant systems for backup of material, et cetera, are they held to a particular licensing standard or a degree of education? Is there some kind of a professional path, or do they just have a nice white business card with a nice emblem and their name is printed in gold?

Ms. D'AGOSTINO. We don't really have any information. We didn't do any work on that. I think in some cases, as was relayed to us, the backup or alternate providers of telecommunications actually did have at one time separate lines and paths; but then later after the contract, sometime later and without notifying the client, moved the paths into the same lines as Verizon.

Mr. MANZULLO. That would be a breach of contract, as far as I am concerned.

Ms. D'AGOSTINO. We—

Mr. MANZULLO. That is none of your—but that is extremely serious, because the companies hired to do this are—boy, I woke you government employees up there, didn't I? Everybody is nodding and saying yes.

I don't have a very technical background and don't understand a lot of these terms that are used in communications, but I just—what I see here is a good-faith effort on the part of these houses to back up their system. You don't anticipate an emergency such as September 11, but they do anticipate somebody getting into their system and screwing up their lines. They do anticipate, you know, a flood or water getting into the basement, or a lightning strike, or a surge, or a fire on their premises.

Here in good faith they hire these firms, and initially, as you said, there are separate lines. Then the lines get merged by the security firms. I consider that to be a very serious breach, and there has to be a tremendous amount of responsibility that is placed upon those companies before setting up a system like that.

You don't have to respond to that. This is more of a comment.

Mr. COLBY. I would just say this is something that came as a surprise to many, including the firms that believed that they had built redundancy. Apparently, as Davi said, they contracted for dif-

ferent systems. They were told by the contract providers what the routes were. The routes were different when they contracted for them, but apparently there was a freedom under the contracts to subcontract, and sometimes in the course of the subcontracting, they got routed through paths that were not diverse—but now steps have been taken to help address this. One includes development by the Securities Information Automation Corporation of its own network. Bob Britz, who is testifying later, is a co-president of that organization and may be able to give you more information on that.

But realizing in hindsight this was a problem, there have been proactive steps taken to create diverse alternatives to the existing telecommunications—

Mr. MANZULLO. But it would be hindsight by the houses. They are not charged with that type of knowledge, and certainly how could it be hindsight by the people putting in the security systems when it does not take but a second grade education to figure out that you have a separate path? I am a pilot, I am not current in my license, but in large aircraft you always have a redundancy system so if something breaks down, you can go onto something else without depending upon those lines.

Maybe I am being hard on these companies, but perhaps I am not. If you contract for security, and you get two lines, and then somebody brings those two lines into one to save some money, I just think that is a very serious breach of ethics. Thank you.

Chairman BAKER. Thank you, Mr. Manzullo.

I do appreciate your appearance here today, the work you have done, but also wish to make it clear that from the committee perspective we understand this is an ongoing and continual responsibility.

In the scope of your services if you identify things that the Congress should respond to, whether it be legislative authority, and certainly matters relating to necessary funds to conduct these activities, the committee would like to continually be informed of those needs so we may be appropriately responsive. We certainly don't want to do anything that contributes to exacerbating a very difficult circumstance when this eventually may reoccur. Thank you very much for both being here.

At this time, I would ask that panelists from the second panel come up to the table. Good afternoon and welcome. I certainly appreciate each of your appearances here this afternoon.

In order to move us along, I would begin by introducing our first witness, Mr. Richard Ketchum, President of the NASDAQ. We certainly welcome your participation here this afternoon.

STATEMENT OF RICHARD G. KETCHUM, PRESIDENT, NASDAQ STOCK MARKET

Mr. KETCHUM. Thank you, Mr. Chairman. Thank you, members of the subcommittee. I want to congratulate you on having this hearing. It is clearly timely, and I think the oversight this committee provides on this critical issue is very, very important. I appreciate this opportunity to describe the steps that NASDAQ has taken to ensure our business continuity in the event of another catastrophic event.

Any analysis of industry preparedness must first review the market's response to the 9/11 attacks. Because our main and backup technology centers are located outside Manhattan, it is important to note at the outset that at no time following the disaster that occurred on September 11 were NASDAQ's systems inoperative. At the time of the 9/11 attacks, trading was suspended, but NASDAQ systems and network continued to operate, and indeed provided an opportunity for testing for the firms that operate in our marketplace. Therefore, our primary concern regarding reopening the markets after 9/11 related to our ability to connect with the firms that are active in NASDAQ and bring liquidity and ordered flow to our marketplace.

Following the 9/11 attack, we worked closely with the SEC, Treasury, Federal Reserve, the NASD and the New York Stock Exchange, as well as key member firms, to resume trading as soon as possible. That cooperation was an important factor in reopening the markets and restoring investor confidence. I am very proud of the efforts of so many talented people at NASDAQ who worked tirelessly with so many others in the financial services community to bring our markets back on that Monday, 9/17, safely and without incident.

While the events of September 11 did not fundamentally change NASDAQ's understanding of the potential range of threats to the financial services sector, they amplified awareness of the potential reach that could be exerted by such threats. NASDAQ has implemented a fully developed business continuity disaster recovery plan that will allow the continued trading of NASDAQ securities in the event that one of the NASDAQ data facilities is rendered inoperative.

In short, we believe that disasters are managed not only by hardening potential points of failure, but also by building redundancies wherever possible into the entire trading network, and by regular testing of those backup capabilities.

Geographic diversification of redundant facilities is a core component of NASDAQ's business continuity strategy. Our redundant data facilities are located hundreds of miles from one another in differing geologic and climatic zones, so that the same natural event has a low likelihood of impacting both sides. NASDAQ also decreases its vulnerability by operating from separate utilities and local telecommunications services.

While we are confident that our system's designs and contingency plans contain appropriate levels of redundancy, NASDAQ appropriately works with member firms to support them in enhancing their backup capabilities as well. In that connection, NASDAQ, working with the NASD, has submitted a ruling filing, as has the New York Stock Exchange, that would require broker/dealers trading in NASDAQ securities to engage in appropriate business continuity planning. As a result of each of these ongoing efforts, I am sure that our equities markets are more resilient than they were on September 11, 2001.

We have also worked closely with the GAO as it evaluated NASDAQ's preparedness and developed its findings and recommendations. We generally share their view on the need to develop goals, strategies, and sound practices to improve the resil-

iciency of trading functions and enhance the SEC's funding for technology and staff.

We are also working with the SEC and the New York Stock Exchange to develop a plan under which NASDAQ and the New York Stock Exchange can trade each other's securities in the event of a disaster that rendered either market inoperable.

It is important to emphasize that these plans are only a final layer of protection for the U.S. Securities markets. The first line of defense for stock markets will always be their own backup systems, and the continued operation of each market has to be the first priority.

In conclusion, following September 11, the U.S. Financial industry demonstrated its resilience and resolve to maintain the most liquid and stable markets in the face of terrible challenges. Truly, NASDAQ's trading network has demonstrated its unique value as part of that infrastructure. However, our work is not done. NASDAQ, the government, and the financial services industry will need to continue to work in concert to ensure that trading can resume following a catastrophic event.

Thank you again for providing me this opportunity to describe the steps NASDAQ has taken, and I would, of course, be happy to answer any questions from the committee.

Chairman BAKER. Thank you, Mr. Ketchum.

[The prepared statement of Richard G. Ketchum can be found on page 278 in the appendix.]

Chairman BAKER. Our next witness is Mr. Robert Britz, president and chief operating officer, New York Stock Exchange.

STATEMENT OF ROBERT G. BRITZ, PRESIDENT AND CO-CHIEF OPERATING OFFICER, NEW YORK STOCK EXCHANGE

Mr. BRITZ. Thank you, Mr. Chairman. I appreciate the opportunity to be here before you and before the distinguished members of this committee.

As the president of the Exchange, I lead the Exchange's Equities Group, which is responsible for the day-to-day operation of our trading floor, our data processing sites, our technical infrastructure, software development, and our information business. I also head the Exchange's International Group, which is responsible for maintaining relationships with international non-U.S. Companies, as well as securing new non-U.S. Listings.

In addition to that, I am chairman and CEO of the Securities Information Automation Corporation, or SIAC, which has been referred to once or twice already today.

On behalf of the NYSE and our chairman, Dick Grasso, I thank the subcommittee for providing this forum to discuss business continuity and contingency planning in conjunction with the release this afternoon of the report of the GAO on that issue.

The report released by the GAO today is the result of more than 17 months of work that included reviewing business continuity plans and the physical and information security measures of the NYSE and SIAC. GAO conducted a dozen visits and follow-up telephone calls with us. We would like to thank the GAO staff for their professionalism throughout this important review.

The NYSE has developed forward-looking business continuity strategies that harden our physical and information technology infrastructure and improve our ability to withstand or recover from a disaster.

Our approach consists of three components: to prevent an attack or natural catastrophe, to withstand them, and to recover from them. In close cooperation with Federal, State, and local law enforcement, the Exchange has expanded its physical security perimeter. We have also taken measures to increase the screening of all people, package delivery, and mail that enters the NYSE or our data centers, and we have instituted a more restrictive policy on visitors and deliveries.

The NYSE employs a rigorous information technology structure to ensure the reliability of all information we receive, process, and disseminate to the world every day. We employ external perimeters, firewalls, intrusion detection, and international access controls, and we conduct penetration testing using so-called friendly hackers.

SIAC chairs the Financial Services Information-Sharing Analysis Center, which was referred to earlier, and that works with government agencies to identify and assess potential threats. All of our facilities have emergency generator backup and store water on site to enable continued operations after the loss of power or water. If we lose natural gas service, we can operate on fuel oil.

Our primary trading floor is actually five distinct trading floors located in four different buildings. Trading can be moved from one location to another as may be necessary, a so-called compaction exercise.

Our plans include redundant, active data centers served by different power grids and multiple telecom central offices, with each site sharing the daily processing load generated by trading about 1.4 billion shares a day. All of our facilities have backup power generators and UPS. We have a backup trading floor that was instituted post-9/11, developed at a cost of approximately \$25 million. This alternative venue would support the trading of all NYSE-listed securities in a very conventional market structure model on a next-day basis after an event that disabled the primary trading floor.

The NYSE and SIAC have launched Secure Financial Transaction Infrastructure, SFTI. That has been referenced once or twice already today. It is a primary extranet servicing the financial industry. It provides diverse, fully redundant routing to the SIAC data centers for member firms, national market participants that are connected to the NYSE, to the American Stock Exchange, the National Market System, and DTCC's IT infrastructure as well.

Following September 11, 2001, U.S. equity trading was interrupted because many broker/dealers lost their connectivity to the markets due to the damage suffered by a major central telecommunications switching facility at Ground Zero. SFTI addresses this by enabling member firms to connect to the NYSE's data centers via private fiberoptic connections to multiple access centers, so-called carrier hotels, throughout the New York metropolitan area, as well as in Boston and Chicago.

SFTI possesses no single point of failure. All of SFTI's equipment, connections, power supplies, network links, and access centers are redundant, and its architecture features independent, self-healing fiberoptic rings. If a SFTI fiber pathway is compromised, financial data traffic is simply rerouted.

The NYSE is ready to trade the top NASDAQ stocks, approximately 250, which account for, we believe, 80 percent of the average daily volume in the unlisted market. All NYSE systems have been modified and can support the four character symbols used by such unlisted stocks so that there is no need for modification of the broker/dealer systems. Because the NYSE's capacity is today about five times our average daily volume, the incremental volume associated with trading these NASDAQ stocks can well be absorbed.

The NYSE is committed to ensuring that the U.S. capital markets remain the envy of the world, and to insulate them from interruption by attack or natural catastrophe by protecting them from threats, by creating an infrastructure that can withstand attack or catastrophe, and by developing contingency plans that enable quick recovery.

In the event a terrorist attack or catastrophe achieves penetration and takes out our real-time infrastructure, the NYSE is able to resume trading in a timely, fair, and orderly fashion that will ensure that every single one of America's 85 million investors has access to our member firms and to us.

Mr. Chairman, I want to thank you for the opportunity to present this testimony, and I would be happy to answer any questions you or the committee members may have.

Chairman BAKER. Thank you, Mr. Britz.

[The prepared statement of Robert G. Britz can be found on page 40 in the appendix.]

Chairman BAKER. Our next participant is Mr. Donald Kittell, executive vice president, Securities Industry Association.

**STATEMENT OF DONALD D. KITTELL, EXECUTIVE VICE
PRESIDENT, SECURITIES INDUSTRY ASSOCIATION**

Mr. KITTELL. Thank you, sir. Thank you, Mr. Chairman and Ranking Member Kanjorski, and members of the committee. I appreciate the opportunity to describe for you the significant progress that securities firms have made in response to 9/11.

The most significant outcome of 9/11, in my mind, was the realization that we are under attack. 9/11 did not occur in our own backyard, it occurred in our own front yard. What has been the impact of that realization? We now know that the danger is real. We assume that additional attacks will happen. We are sensitive to the expanded range of potential scenarios impacting both physical and cybersecurity that exist. We agree with the comments of the earlier discussion about cybersecurity.

We have established industry command centers which are linked with other centers in municipal, State, and Federal Government, homeland security, as well as other industry sectors. We are engaged in a long-term strategy to disperse industry infrastructure. We are making significant investments in effective backup facilities which are currently being tested. We have recognized that disaster recovery is the responsibility of the entire enterprise of a firm and

not just its information technology or operations groups. We recognize that we are dependent on external critical service providers, such as telecom, transportation, power, and municipal services such as police and fire.

We cannot say that we can defend against any and all attacks; we can say that we understand the threat and have taken significant steps towards prevention and recovery.

I would like to highlight three aspects of the industry's efforts. First, the financial services sector is sharing resources through the Financial Services Sector Coordinating Council. This group represents over 20 trade associations and industry organizations, many of whom did not speak to each other prior to 9/11, but are now sharing continuity planning resources.

An example of the effectiveness of this group is the coordination of efforts across the sector with financial services regulators, so we have 15 financial services regulators with a single point of contact to 20 or more industry associations.

A third example is the coordination of the Financial Services Information Sharing and Analysis Center, which Bob Britz just talked about, which addresses cybersecurity attacks, which gives us the ability to communicate with each other in a rapid fashion.

The second important aspect I would highlight is the positive relationship between the private sector and the financial services sector. This relationship was remarkably effective in the immediate response to 9/11, and it continues to be so in the industry's efforts to strengthen resiliency over the last year and a half.

An example of that is the dialogue on the Financial and Banking Information Infrastructure Committee, or FBIIC, that Bob Colby referred to earlier; the financial services regulators, chaired by the U.S. Treasury and the FSSC that I referred to earlier representing the private sector.

The second example is the white paper dialogue between the regulators and the industry on clearance and settlement infrastructure, which was discussed earlier. There were actually two papers on clearance and settlement, both which raised significant questions and industry participants referred to with thoughtful comments. There is continuing dialogue on this. I think Mr. Colby said the next version of the second white paper would be out within a month, and we look forward to continuing that dialogue with the regulators.

The third important aspect that I would highlight is the positive contribution of the GAO. We worked with the GAO, notably on Y2K 2 years ago. We found their input to be extremely constructive. We have had the opportunity to review a draft of the report released today, and although I have not had the opportunity to review this with our member firms, I do want to make the following comments.

First, we agree with the GAO findings that business continuity plans need to be improved over the pre-9/11 status. I also note that the period of the GAO study was, I believe, February to June of 2002, and a great deal has happened since that time.

We also agree with the specific areas for improvement highlighted in the GAO report, such things as improved backup facilities, greater geographic dispersion, and so on.

Secondly, SIA agrees that the clearance and settlement facilities are critical to an effective resiliency plan. We forwarded our comments on the white paper, and we are very pleased with the results so far of the organizations involved in clearance and settlement.

We also agree with GAO that the trading facilities are also critical to an effective resiliency plan. There is no better example than the effort to open the market following 9/11.

We also agree with the SEC's comments that the regulatory environment around the trading function is different than the regulatory environment around clearance and settlement. However, we are very confident that those issues can be resolved, and that the firms certainly do not believe that there should be any less emphasis on trading facilities than on clearance and settlement.

Finally, SIA supports additional funding for the SEC as a general matter, but particularly including its oversight of business continuity.

The securities industry has built on its commitment to operational recovery, its experience on Y2K, and other industrywide projects to effectively address the threats posed by terrorist attacks. The efforts of individual organizations, the coordination of activities across all the sectors in the financial services sector, the positive relationship with the regulators, with the oversight of the Congress and the GAO, is a strong combination for an effective response to terrorism.

We have accomplished a great deal in the last year and a half. We understand there is more to be done. We are committed to the task ahead.

Thank you.

Chairman BAKER. Thank you very much, sir.

[The prepared statement of Donald D. Kittell can be found on page 290 in the appendix.]

Chairman BAKER. Our next witness is Mr. Micah Green, president of the Bond Market Association. Welcome, Mr. Green.

**STATEMENT OF MICAH S. GREEN, PRESIDENT, THE BOND
MARKET ASSOCIATION**

Mr. GREEN. Thank you, Mr. Chairman and Mr. Kanjorski.

Mr. Chairman, I want to thank you for the opportunity for us to give our testimony, and really congratulate you for the leadership you have shown on this issue, and for the work of the SEC and other regulators in working with the industry to try to move on this important issue.

I will touch briefly on the business continuity issue, but want to spend most of my oral remarks telling you about the bond markets and how they responded at the time of 9/11, beyond, and then looking to proposals that could affect the future.

Briefly on business continuity plans, I would frankly associate myself with the remarks of Mr. Kittell. We have worked very closely with the SIA to provide the bond market perspective on the issue of business continuity, and we have been participating in the coordinating councils.

We, too, have set up a management council within our organizations working with our members to create redundancy, and frankly working within the association to create the ability to communicate

with our membership, because what we learned at that time is that communicating within the breadth of the industry was almost as important as the industry itself communicating with its customer base. So I would really stand by what our colleagues at SIA said about business continuity planning.

But let me relate it to the bond markets, because the bond markets are very different in the way they operate versus the equity market.

Unlike the centralized, exchange-traded New York Stock Exchange and other equity markets, the bond markets are inherently a decentralized, over-the-counter market, which means it is a dealer-to-dealer marketplace. People buy and sell bonds when they want to buy them, where they want to buy them. There are hours of trading, but frankly, it is a 24-hour marketplace.

The New York marketplace right now is starting to wind down. The Japan and other Asian marketplaces are starting to crank up. About 11 hours from now, the London and other European markets will crank up. It is a never-ending cycle.

In fact, an interesting thing to remember in 9/11, much of the trading that occurs in the bond markets, particularly in the repurchase agreement market, which is the funding mechanism for many of the trades, actually occurs before 9 o'clock in the morning. So when that first plane hit the World Trade tower at 8:46 a.m. And hit the largest inter-dealer/broker of all, Cantor Fitzgerald, there were hundreds of billions of dollars of transactions that had already occurred that day.

In fact, daily volume in the bond markets is over \$600 billion a day. There are almost \$20 trillion of bonds outstanding, and it is a very actively traded market. So when those planes hit, it was not just about getting the markets back open; it was also about figuring out what took place that went down with those towers, so the effect on the clearance and settlement process. And figuring out how to get the bond markets back open was as much about trying to reconcile what had occurred so those trades could be completed and those trades could be closed.

Interestingly, while the stock markets were able to open up through these heroic events on Monday, September 17, the bond markets, because of their decentralized character, were able to get back up and running on an orderly basis at 8 a.m. on Thursday morning, September 13. Interestingly, though, bonds never stopped trading. There were trades done in the afternoon of 9/11. The Fed, the Federal Reserve, in its exercising of monetary policy, came to the marketplace to provide liquidity to the marketplace in the government securities market on 9-12.

So, as you see, the bond markets can operate differently. Because of their role in the financial system, keeping markets open is crucially important.

It is a good segue into a proposal that is now pending coming out of the Municipal Securities Rulemaking Board in their post-9/11 efforts. They have recommended to grant them the authority—the Municipal Securities Rulemaking Board, a self-regulatory organization governing just the municipal securities market—to grant them the authority in the case of an emergency to, by regulation, halt trading in those markets.

The reaction of our association has been one of strong opposition to that, because we believe, frankly, in the time of an emergency is when you want markets open. You want capital to flow as smoothly and as easily as possible, so we oppose it philosophically.

We do understand, though, that policymakers such as yourselves or the SEC or other regulators may want some degree of authority if the worst, the unthinkable, God forbid, ever happens again, much worse than 9/11. So the Bond Market Association, while we have a philosophical opposition to a self-regulatory organization, or frankly, any authority, saying decentralized debt markets should be halted by law, we realize you may have an interest in having some Federal authority.

We could live with a governmental authority, not a self-regulatory authority but a governmental authority, at the highest possible level to deal with emergencies—we can't tell you what authority that is because of the unique nature of the regulatory scheme covering the bond markets generally, frankly—working with the President's Working Group, which includes the SEC, the Treasury, the Fed, including the Chicago markets, so that there is a coordinated response, and that authority should be narrowly defined so that it is absolutely under a severe catastrophe. It is not about a breakdown of any computer system or a breakdown of any trading system, but it really has to be a catastrophe, because in times of stress, we need markets open. In times of stress, we need capital to flow. Because of the unique, decentralized nature of the bond markets, they are able to more naturally operate in those circumstances. We believe they should be open as much as possible.

That would really conclude my oral remarks. I would be happy to answer any questions you would have.

Chairman BAKER. Thank you, Mr. Green.

[The prepared statement of Micah S. Green can be found on page 185 in the appendix.]

Chairman BAKER. I would ask the counsel and members, my side has pretty much decided. I have just a few questions that I would pose for the record for a written response. Mr. Kanjorski may have a comment or two.

In order to use our time efficiently, I would conclude our hearing, because we have a series of three votes which would keep us for a bit.

Does anyone have any objection?

Mr. Kanjorski?

Mr. KANJORSKI. No, Mr. Chairman.

Chairman BAKER. If I may, let me just pose a few questions.

Also, the record will remain open for Members to, in writing, submit further inquiries at their leisure. That certainly would be preserved.

Chairman BAKER. Mr. Scott, do you have any comment?

Mr. SCOTT. Just one question, sir.

Chairman BAKER. One second, and we will try to get to you.

I noted in the GAO report, Mr. Britz, that there is a comment that the SEC has asked the New York Stock Exchange and NASDAQ to take steps to ensure their information systems can conduct transactions and securities that the other organizations trade. However, under this strategy the 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 exchange's deals.

Given our time constraints, I don't expect a discussion on it at the moment, but if you can address that section of that report and tell us what is planned; or perhaps since the date of the report has that been addressed.

Secondly, I would like each of your opinions concerning the GAO's observation that the SEC did not make mandatory the ARP program rules, but expected the changes that they recommended and the clearing organizations to comply with the various information technology and operations practices voluntarily.

I would like to get back from you a statement if there is a problem with mandatory compliance, the reasons therefore; or if there isn't, is there some general review by your respective bodies as to when or if the SEC should adopt such mandatory compliance?

And then thirdly, the presentation of the white paper expected in a month, I don't know if we will have another hearing on the matter, but certainly we would like to have industry communication to us about the outcomes of modifications made and agreements reached as a result of the next white paper.

Chairman BAKER. Mr. Kanjorski.

Mr. KANJORSKI. Mr. Chairman, I want to congratulate the panel for a great report to us.

The only thing, Mr. Britz, I recently visited the chairman's office in October. I am worried about the electronic controls on the thermostat.

Chairman BAKER. Mr. Scott.

Mr. SCOTT. One of the things—one of the conclusions that was reached in a report released today was the length of time that our markets could stay down, that we could absorb certain lengths of times. I want to say with that how proud I think all America was that we were able to get back up and running so quickly after that devastating hit. But it did go on to say that there is a certain amount of time before the economy will be affected.

Do we have any idea of how long that delay would be before the economy is really affected in terms of days, that it would be negatively affected?

Mr. BRITZ. I am not an economist, Congressman, so I would be very loath to say it is 2 days, 4 days, or 6 days. I will say, coming out of 9/11, we were down from the 11th until the 17th. If we were to have the same kind of circumstance occur again, I am very confident that our markets would be up in a day or two; or let me put it this way, technically they would be able to be up in a day or two. There may be policy considerations as to why that is not a good idea.

From an infrastructure point of view, I think we have put in place the kind of backup and contingency planning and infrastructure that would not give rise to the 4- or 5-day kind of outage that we had on September 11, 2001.

Mr. GREEN. I would just add that if the system of payments is affected, Congressman—and, for example, if the Federal Reserve cannot come to market to add liquidity because the marketplace is closed, that has an immediate effect on the macroeconomy. But in

the microeconomy, an investor who wants to sell security because they need cash to pay a kid's tuition bill, that affects them immediately when they need that money, so you need to open markets as quickly as possible.

Chairman BAKER. Thank you each for your participation. There will be further follow-up questions in the offing, but we do request your continued information flow to the committee to help us understand our circumstance. Thank you.

[Whereupon, at 4:53 p.m., the subcommittee was adjourned.]

A P P E N D I X

February 12, 2003

Statement of the Honorable William Lacy Clay before the Sub-committee on Capital Markets,
Insurance, and Government Sponsored Enterprises, Committee on Financial Services

"Protecting the Capital Markets Against Terrorism"

THANK YOU, MR. CHAIRMAN. I WELCOME THE OPPORTUNITY TO MEET WITH THE COMMITTEE TODAY. I THANK THE WITNESSES FOR BEING HERE TO SHARE THEIR KNOWLEDGE AND EXPERTISE. THE PURPOSE OF THE HEARING IS AMONG THE HIGHEST PRIORITIES THAT WE MAY HAVE AS A COUNTRY. WE HAVE TO EXAMINE THE FACTORS THAT SHOULD BE CONSIDERED IN ASSESSING THE RISKS OF TERRORISM AND THE IMPACT ON OUR CAPITAL MARKETS.

JUST A SHORT TIME AGO, THIS SUBJECT WOULD HAVE BEEN AS SERIOUS, BUT WOULD NOT HAVE THE URGENCY AND THE KNOWLEDGE THAT THIS HAS TO BE ADDRESSED AND ACTED UPON POST HASTE. SEPTEMBER 11, 2001 CHANGED ANY PERCEPTION THAT TERRORISM ON AMERICAN SOIL WAS ONLY A POSSIBILITY. IT IS NOW A PROBABILITY AND A REALITY. THE THREAT IS REAL. IT WILL REMAIN REAL FOR THE FORSEEABLE FUTURE. THEIR MANAGERS OF OUR FINANCIAL MARKETS NEED BOTH PROCEDURES FOR ACTIONS AND THE KNOWLEDGE OF HOW TO IMPLEMENT THOSE PROCEDURES THAT ARE ESTABLISHED. THE AMERICAN PEOPLE NEED TO HAVE THE CONFIDENCE THAT THEIR SECURITIES ARE SAFE.

I APPLAUD THE EFFORTS OUR SECURITIES FIRMS HAVE TAKEN TO MAKE SURE THAT OUR MARKETS ARE PREPARED TO RECOVER FROM FUTURE DISASTERS.

I WILL END MY STATEMENT AT THIS POINT AS I AM EAGER TO HEAR FROM OUR WITNESSES WHAT SAFEGUARDS WE HAVE IN PLACE AND WHAT ADDITIONAL ASSISTANCE, IF ANY, IS NEEDED TO ACCERTAIN THAT OUR MARKETS ARE SECURE.

MR. CHAIRMAN, I ASK UNANIMOUS CONSENT TO PLACE MY STATEMENT INTO THE RECORD.

DISTRICT OFFICE:
150 MOTOR PARKWAY, SUITE 108
HAUPPAUGE, NY 11788
PHONE: (631) 951-2210
PHONE: (516) 505-1455
FAX: (631) 951-3308



WASHINGTON OFFICE:
429 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
PHONE: (202) 225-3335
FAX: (202) 225-4609

Congress of the United States
House of Representatives

STEVE ISRAEL
Second District, New York

Mr. Chairman, thank you for holding this very important hearing.

Let me begin by saying that many of the people who helped get the markets back in order after the September 11th attacks are my constituents. They worked tirelessly and creatively to implement business recovery plans and to get our economy moving again. Record volumes occurred when the markets re-opened and there was not a blip that the ordinary investor could see. I think we should begin by commending the people at the exchanges, regulatory agencies and banks, brokerage houses and other firms that made it all work.

These same people, I fear, are going to be called upon again to implement their contingency plans. But the question is: are we planning for the contingencies of this new era?

I have been concerned for some time not only about conventional threats to our nation, but the unconventional threats. We know that we can respond to a natural disaster. We know that we can respond to the horrors of September 11. But what if there was a massive cyber attack on the settlement systems in our financial systems? A trading day would have occurred, but when it came time to settling the books, all of the data was lost. People who bought and people who sold might never know if their transactions went through. Billions of dollars could be lost. More importantly, the long-term damage to our system would be devastating. This is but one example of cyber-terrorism that we must anticipate.

I am sure I am not alone in fearing worst-case cyber-scenarios. But are we planning for them? Are we testing for them? Are our CEO's and CFO's focusing on this? I believe that this is a problem on a par with the Y2K problem we faced several years ago. Then, the public and private sectors came together in incredible cooperation and beat the bug. Do we have the same commitment today? I would submit that we better get that level of commitment.

Mr. Chairman, I am told that we may have more hearings in the future about such issues. I look forward to those and I look forward to hearing from our witnesses about their work.

**OPENING STATEMENT OF
RANKING MEMBER PAUL E. KANJORSKI
SUBCOMMITTEE ON CAPITAL MARKETS, INSURANCE,
AND GOVERNMENT SPONSORED ENTERPRISES
HEARING ON RECOVERY AND RENEWAL:
PROTECTING THE CAPITAL MARKETS
AGAINST TERRORISM AFTER SEPTEMBER 11
WEDNESDAY, FEBRUARY 12, 2003**

Mr. Chairman, before we begin, I must note that this hearing is the first meeting in the 108th Congress of our subcommittee. Over the last eight years, we have forged a close and productive relationship as the Chair and Ranking Member of the Capital Markets Subcommittee.

Moreover, our subcommittee during the last two years sat at the center of the eye of the storm on two significant pieces of legislation: creating a federal backstop for terrorism reinsurance and restoring investor confidence in corporate America. We performed our jobs admirably on each of these matters, and I look forward to working with you once again in this Congress on these and other important issues.

Today, we will hear from a variety of witnesses about the response of our regulators and key market participants to the September 11 attacks. These attacks resulted in the unfortunate loss of nearly 2,800 lives at the World Trade Center. They also resulted in excess of \$40 billion in insured damages, according to at least one estimate.

In my view, our country cannot -- and must not -- allow terrorists to alter the effective functioning of the U.S. financial markets, the strongest in the world. Fortunately, the participants in our capital markets demonstrated the resiliency of our system. The fixed income markets successfully resumed trading just two days after the attack, and our equities and options exchanges reopened six days after the attack.

At today's hearing, we will hear from a number of distinguished witnesses, including representatives from the General Accounting Office, the Securities and Exchange Commission, the New York Stock Exchange, and the Nasdaq Stock Market. We will also hear from the Securities Industry Association and the Bond Market Association. These witnesses will provide us with a valuable perspective in understanding the health of the financial services industry and the need for any changes in public policy in the wake of the September 11 disaster.

In particular, I am interested in hearing the testimony of the GAO. The GAO recently completed a comprehensive examination of the preparations that our financial market participants have taken since September 2001 to protect themselves from physical and electronic attacks. In general, the GAO found that while our capital markets have implemented a number of reforms to improve business contingency planning, additional action is needed to better prepare critical financial market participants.

As we consider today the issue of contingency planning in response to future terrorism events, our panel should also consider other potential threats to our capital markets. In 1998, for example, financial regulators responded in an improvised manner to the collapse of Long Term Capital Management. In order to promote domestic economic security in times of turmoil, we

need for financial and economic regulators, as well as market participants, to better coordinate their efforts to respond to economic crises in advance of such events. I was therefore pleased that the Committee adopted my amendment regarding this issue to the oversight plan. I intend to continue to examine this issue in the months ahead.

Finally, Mr. Chairman, it is important that this Congress act promptly on one piece of legislative business related to these matters -- the Emergency Securities Response Act. To facilitate the reopening of our capital markets, the SEC for the first time used its emergency power authorities to ease temporarily certain regulatory requirements. Nonetheless, the SEC recommended some statutory improvements to these authorities. Although the House approved legislation adopting these reforms, it did not become law in the last Congress. It is nonetheless my hope that this bill will become law in the near future.

Mr. Chairman, thank you again for the opportunity to comment on these matters. I look forward to continuing our cooperative relationship in the 108th Congress, and yield back the balance of my time.

CAROLYN B. MALONEY
14TH DISTRICT, NEW YORK
2450 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-3214
(202) 225-7944
COMMITTEES:
FINANCIAL SERVICES
GOVERNMENT REFORM
JOINT ECONOMIC COMMITTEE



Congress of the United States
House of Representatives
Washington, DC 20515-3214

DISTRICT OFFICER:
1051 THIRD AVENUE
SUITE 211
NEW YORK, NY 10158
(212) 850-0606
 28-11 ASTORIA BOULEVARD
ASTORIA, NY 11102
(716) 932-1804

Statement of Rep. Carolyn B. Maloney
February, 12 2003

"Recovery and Renewal: Protecting the Capital Markets Against Terrorism Post-9/11"

Thank you, Chairman Oxley and Chairman Baker, for holding this hearing on protecting the capital markets and the economy from another terrorist strike.

It is highly appropriate that we review the findings of the GAO as to the level of preparedness of the markets. I agree, prudence demands that backup systems be in place in the event of another attack. However, I want hope we take care to ensure that Congress and the federal regulators not unnecessarily force financial services firms to move jobs out of New York City as we review preparedness.

Recently, the financial services regulators issued a "Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System." I continue to be concerned that the implementation of this white paper could result in the relocation of thousands of workers and significant physical resources of major financial institutions out of New York and to locations across the country.

Experience dictates that existing financial services firms' contingency planning is fairly well in place. The 9/11 attacks caused unprecedented damage in the center of New York City's financial district. Despite this extraordinary damage, markets reopened within a number of days. Many of the existing contingency plans were put in place for Y2K. Given this existing investment in backup systems

I think there are questions about the need for formal guidance that firms should move additional operations to out-of-region facilities hundreds of miles away from New York or other financial centers.

As a bottom line I share the goal of maintaining the continuity our economy in the event of an attack. I only request that policymakers tread very carefully and not cause additional damage to the future of the New York City economy. I yield back the balance of my time.

Opening Statement
Congressman Ed Royce (CA-40)
12 February 2003
"Recovery and Renewal: Protecting the Capital Markets
Against Terrorism Post-9/11"

Thank you, Chairman Oxley and Chairman Baker, for providing the Members of this Committee with the opportunity to address our domestic financial markets' ability to respond to every American's worst nightmare -- another catastrophic terrorist attack on the United States.

Yesterday, the Wall Street Journal outlined the results of a war game, dubbed "Dark Winter" and run by the Johns Hopkins Center for Civilian Biodefense Strategies, which poses a realistic scenario in which a bioterror attack on the United States leads to an outbreak of smallpox, causing serious domestic disruption and eventually spreading this contagion across 10 other countries.

The results of this war game serve to underscore the fact that while the United States is making a great deal of progress in the War on Terror, we are still unacceptably vulnerable to an asymmetrical attack on "soft" targets like our civilian population, our food supply, and our financial markets. I commend the Chairman for his foresight in requesting that the GAO undertake a comprehensive examination of the preparations that financial market participants have taken since September 11 to protect themselves from physical and electronic attacks.

While I strongly believe that the creation of our new Department of Homeland Security will mitigate or ameliorate many of the threats that the United States currently faces, it is incumbent upon all of us to do our part to ensure that the United States and our financial infrastructure can cope with another terrorist attack so that the American way of life and commerce will be interrupted as minimally and briefly as possible. I appreciate the efforts that have already gone into making Americans safer, and I look forward to finding new ways to protect Americans from the threats of this new age.

I would like to thank our witnesses from both the GAO and from the non-governmental sector for their work in briefing this Committee on their current and future efforts to defend our financial markets from acts of terror. I also look forward to working with the Chairman on developing ways to make our financial markets more secure and less vulnerable to attack, and I yield back the balance of my time.

Testimony

New York Stock Exchange, Inc. 11 Wall Street New York, NY 10005 www.nyse.com



Robert G. Britz

Executive Vice Chairman, President and Co-Chief Operating Officer
New York Stock Exchange, Inc.

On

“Recovery and Renewal: Protecting the Capital Markets
Against Terrorism Post 9/11”

Subcommittee on Capital Markets, Insurance and
Government Sponsored Enterprises

Committee on Financial Services
United States House of Representatives
Washington, DC

February 12, 2003

Robert G. Britz

Executive Vice Chairman, President and Co-Chief Operating Officer

New York Stock Exchange, Inc.

On

Recovery and Renewal: Protecting the Capital Markets Against Terrorism Post 9/11

Committee on Financial Services

Subcommittee on Capital Markets, Insurance and Government Sponsored Enterprises

United States House of Representatives

Washington, DC

Wednesday, February 12, 2003

I. Introduction

Chairman Baker, Congressman Kanjorski and distinguished Members of the Subcommittee, I am Robert G. Britz, Executive Vice Chairman, President & Co-Chief Operating Officer of the New York Stock Exchange, Inc. ("NYSE" or "Exchange"). I lead the Exchange's Equities Group, which is responsible for the day-to-day operation of our Trading Floor and our

data processing sites, for our technical infrastructure and software development and for our information business. I also head the Exchange's International Group, which is responsible for developing new NYSE listings of non-U.S. companies. In addition, I serve as the Chairman and CEO of the Securities Industry Automation Corporation ("SIAC"), the NYSE's technology subsidiary.

On behalf of the NYSE and our Chairman, Richard A. Grasso, I thank the Subcommittee for providing this forum to discuss business continuity and contingency planning in conjunction with the release this afternoon of the General Accounting Office's ("GAO") report.

The report released by the GAO today is the result of more than seventeen months of work that included reviewing the business continuity plans, physical and information security measures of the NYSE and SIAC. The GAO conducted a dozen visits and follow-up telephone calls with us. We would like to thank the GAO staff for their professionalism throughout this important review.

II. Business Components

There are seven critical business components required for NYSE trading:

1. The NYSE's Trading Systems - located in two, separate, active data centers that are designed to recover and resume trading intra-day after the loss of one data center;
2. The NYSE's Trading Floor - one primary Trading Floor and one backup Trading Floor located in two New York City boroughs. Trading can resume in less than 24 hours after the loss of the primary Trading Floor;

3. NYSE Member Firm connectivity to the NYSE's information technology infrastructure - required for receiving orders, transmitting quotes and reports and receiving post trade data;
4. Specialist and Member Firm Trading Floor personnel;
5. Market Data Dissemination to the Public - includes SIAC's ability to transmit this data to market data vendors and the vendors' ability to provide it to the public;
6. Liquidity Providers - Upstairs member firm and specialist personnel; and the
7. Clearance and Settlement Processes - these systems are hosted and operated by both SIAC and the Depository Trust Clearing Corporation (DTCC).

III. Critical Infrastructure

The NYSE has a long history of developing forward-looking business continuity strategies that harden our physical and information technology (IT) infrastructure and improve our ability to withstand or recover from a disaster.

All of our facilities have emergency generator backup and store water onsite to enable continued operations after the loss of power or water. If we lose our natural gas service we can operate on fuel oil. We connect our IT infrastructure with a private extranet that utilizes geographically redundant fiber routes. The NYSE and its subsidiaries employ large security forces and invest in automated security systems to protect the infrastructure. Significant investments have been made in information security personnel and infrastructure to protect our systems from intrusions and attacks while enabling our business partners to connect to the NYSE IT infrastructure in a secure manner. Our primary Trading Floor is actually five different

Trading Floors located in four different buildings. Trading can be moved from one location to another as may be necessary.

IV. Contingency Planning

Contingency planning has played a key role at the NYSE for many years. Our plans include redundant, active data centers served by different power grids and multiple telecommunications central offices, with each site sharing daily the processing load generated by the trading of about 1.4 billion shares. All of our facilities have back-up power generators and uninterruptable power source (UPS) systems. All of our facilities are interconnected through a diversely routed private fiber optic network that does not pass through any phone company central office.

We have a back-up Trading Floor, developed at a cost of approximately \$25 million dollars and 30 person years. This alternative venue would support the trading of all NYSE-listed equity securities, without modifications to the NYSE's market structure model, on a next-day basis should an event disable the primary Trading Floor. Support is provided for both specialist and brokers and a full suite of trading applications.

The NYSE has strengthened its physical security in and around the primary Trading Floor at the Exchange's headquarters and our data centers. We are committed to protecting the safety of all personnel at the NYSE. In close cooperation with Federal, state and local law enforcement, the Exchange has expanded its physical security perimeter. We have also taken measures to increase the screening of all people, package deliveries and mail that enters the NYSE or our data centers, and we have instituted a more restrictive policy on visitors and deliveries.

The NYSE employs a rigorous information security infrastructure to ensure the reliability of all information that we receive, process, and disseminate to the world every day. We employ external perimeters, intrusion detection, internal access controls, and we conduct penetration testing by using “friendly” hackers. SIAC chairs the Financial Services Information Sharing Analysis Center (ISAC) that works with government agencies to identify and assess potential threats and to respond to actual threats.

As a self-regulatory organization (“SRO”), the NYSE has filed with the SEC proposed NYSE Rule 446, which would mandate that NYSE member firms specifically define and continuously update business continuity plans. Once approved by the Commission, the NYSE’s Member Firm Regulation Division will review member firm business continuity plans as part of the NYSE’s ongoing and rigorous examination practices.

We have initiated a program to improve coordinated communication with Federal agencies as well as NYSE members and staff. We have created an Emergency Notification System that will forward to our member firms alert messages received from the Department of Homeland Security or the SEC. The Exchange has established new 800 numbers and websites for disseminating emergency information to its members and staff and is developing a secure contingency website for members and staff to report their status after an emergency.

V. Communications Redundancy

The NYSE and SIAC have launched Secure Financial Transaction Infrastructure (“SFTI,” pronounced “safety”), a private extranet to serve the financial industry. SFTI provides diverse, fully redundant routing to the SIAC data centers for the member firms and national market participants that are connected to the NYSE, American Stock Exchange (“AMEX”), National Market System (“NMS”) and DTCC IT infrastructure. Following September 11, 2001,

U.S. equities trading was interrupted because many broker-dealers lost their connectivity to the markets due to damage suffered by a major central telecommunications switching facility at Ground Zero. SFTI addresses this by enabling member firms to connect to the NYSE's data centers via fiber-optic connections to multiple access centers throughout the New York tri-state region, as well as in other financial centers in Boston and Chicago.

Instead of running circuits directly to SIAC, users will connect to multiple Access Centers via their carrier(s) of choice, eliminating the need to rely on a single telecommunications route. Once the communication reaches the Access Center, SFTI will carry the signal to SIAC via geographically and physically diverse fiber route pathways.

SFTI possesses no single point of failure. All of SFTI's equipment, connections, power supplies, network links and Access Centers are redundant and its architecture features independent, self-healing fiber-optic rings. If a SFTI fiber pathway is compromised, financial data traffic will continue to move uninterrupted along another route.

V. Unlisted equities

The NYSE is ready to trade the top 250 Nasdaq stocks, which comprise almost 80 percent of Nasdaq's average daily volume. All NYSE systems have been modified and can support the four character symbols used by such unlisted stocks. Testing with the NYSE's member firms is underway and will conclude in the second quarter. The NYSE will schedule semi-annual production tests with all affected systems to enhance continued readiness to trade Nasdaq stocks. We believe that our current capacity model and our continuing enhancements to our capacity would be adequate. It should be noted that the NYSE's capacity is approximately five times our current average daily volume, which is approximately 1.4 billion shares. With the recent addition of capacity-on-demand from our technology vendors, our capacity is more than

adequate to handle our message traffic as well as the additional message traffic for the top 250 Nasdaq securities.

The NYSE is committed to ensuring that the U.S. capital markets remain the envy of the world. In the event of another terrorist attack or catastrophe, the NYSE plans to resume trading in a timely, fair and orderly fashion that will provide every single one of America's 85 million investors with access to the finest system of enterprise that the world has ever known. We will continue to work with the SEC, the NYSE's member firms, and the entire securities industry to address threats and to implement strategies and solutions. I hope the foregoing is helpful to the Subcommittee. We look forward to working with you and the Financial Services Committee on issues affecting the capital markets. Mr. Chairman, I want to thank you for the opportunity to present this testimony. I would be happy to answer any questions.



**TESTIMONY
OF
ROBERT L.D. COLBY
DEPUTY DIRECTOR, DIVISION OF MARKET REGULATION
U.S. SECURITIES AND EXCHANGE COMMISSION**

**CONCERNING
RECOVERY AND RENEWAL: PROTECTING THE CAPITAL
MARKETS AGAINST TERRORISM POST 9/11**

**BEFORE THE SUBCOMMITTEE ON CAPITAL MARKETS,
INSURANCE, AND GOVERNMENT SPONSORED ENTERPRISES**

COMMITTEE ON FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

FEBRUARY 12, 2003

U. S. Securities and Exchange Commission
450 Fifth Street, N.W.
Washington, D.C. 20549

Recovery and Renewal: Protecting the Capital Markets Against Terrorism Post 9/11

Testimony
of
Robert L.D. Colby
Deputy Director, Division of Market Regulation
U.S. Securities and Exchange Commission

Before the House Subcommittee on Capital Markets, Insurance, and Government
Sponsored Enterprises, Committee on Financial Services
February 12, 2003

Chairman Baker, Ranking Member Kanjorski and Members of the Subcommittee:

I appreciate the opportunity to testify before you today, on behalf of the Securities and Exchange Commission, regarding the efforts since the September 11 terrorist attacks to better protect U.S. financial markets and institutions. My testimony will focus primarily on the steps taken by the Commission and the securities industry to strengthen the resilience of the securities markets over the past 17 months. I also will briefly discuss the Commission's longstanding program to review key automated systems that support the U.S. financial markets. In so doing, I will address, in general terms, issues raised in the Report released today by the U.S. General Accounting Office (GAO) regarding certain additional actions to better prepare critical financial market participants for potential terrorist attacks.¹

I. Resilience of Securities Markets

As the GAO recognizes in its Report, participants in the U.S. financial markets made heroic efforts to recover from the devastation of the September 11 attacks, with the result that all markets reopened successfully within a week after those tragic events. Nevertheless, the Commission, other regulators and the industry have engaged in wide-ranging and intensive efforts to consider the "lessons learned" from the events of September 11, and strengthen the resiliency of the financial sector, so that we are even better prepared going forward.

A. Industry Efforts

Immediately after the September 11 attacks, the securities industry recognized the need to develop more rigorous business continuity plans that address problems of wider geographic scope and longer duration. Market participants have taken a number of significant steps to improve their resiliency, including establishing more robust and

¹ Report to Congressional Requesters of the United States General Accounting Office entitled *Potential Terrorist Attacks: Additional Actions Would Better Prepare Critical Financial Market Participants* (February 12, 2003).

geographically dispersed backup facilities for operations and data recovery, improving crisis management procedures, and seeking telecommunications diversity. Given the highly-interconnected nature of the financial sector, the business continuity efforts of market participants must be coordinated to be effective, and various industry associations have been instrumental in this regard. Last summer, for example, the Securities Industry Association developed a number of “best practices,” relating to business continuity programs, recovery strategies, and recovery resources, that it recommends be observed by all securities firms. In addition, the securities industry has taken concrete steps to reduce its vulnerability to telecommunication failures. The Securities Industry Automation Corporation (SIAC), for example, has developed a private, highly-resilient communications network – known as the “Secure Financial Transaction Infrastructure” or “SFTI” – to offer market participants local connectivity to key trading, clearance and settlement, and market data services.

B. Regulatory Efforts

The Commission and other financial regulators also have been devoting substantial resources to projects designed to strengthen the resilience of the financial sector. For example, the Commission has been working with the Federal Reserve Board and the Office of the Comptroller of the Currency in an effort to identify “sound practices” for business continuity planning for key market participants. This past August, we published for comment a draft White Paper that focused on a small – but critical – group of participants in the U.S. clearance and settlement system. The goal of this project is to minimize the immediate systemic effects of a wide-scale disruption by assuring that the key payment and settlement systems can resume operation promptly following a wide-scale disaster, and major participants in those systems can recover sufficiently to complete pending transactions. In this way, market participants unaffected by the disaster could continue to operate with minimal disruption and, when those impacted by the event are in a position to resume operations, the critical infrastructure would be available for them to do so. The sound practices include intraday resumption or recovery goals, maintenance of sufficient geographically dispersed resources to meet those goals, and routine testing of business continuity arrangements. The agencies expect to issue the final White Paper next month, after an additional round of consultations with the industry, and then incorporate the sound practices into their respective forms of supervisory guidance.

In addition, Commission staff has been reviewing, on an ongoing basis, the efforts of the organized securities markets – the exchanges, Nasdaq, and electronic communications networks (ECNs) – to strengthen their resilience in the post-September 11 environment. As noted in the GAO Report, these markets have taken a variety of steps to improve their physical security, information system protections, and business continuity capabilities. For example, the New York Stock Exchange has taken substantial measures to physically secure its Wall Street trading floor, and has established an off-site alternative trading floor that could be activated on a next-day basis if the exchange’s Wall Street trading floor was rendered inaccessible. Commission staff continues to work with these markets to further increase the robustness their individual

plans. In addition, we have been exploring with the markets the possibility of mutual back-up arrangements. For example, at our urging, the New York Stock Exchange and Nasdaq have agreed to serve as back-up trading platforms for each other's securities if a catastrophic event forced an extended closure of one market. We continue to work with the New York Stock Exchange and Nasdaq as they assess, with key market participants, the optimal framework for these back-up arrangements.

As to the resilience of securities firms, the New York Stock Exchange and NASD have proposed rules that would require all broker-dealers to have business continuity plans that address a number of important areas. Specifically, under the proposed rules, member firms would need to develop, maintain, review, and update business continuity plans which establish procedures to be followed in the event of an emergency or significant business disruption. Among other things, these procedures would have to address data back-up and recovery, mission critical systems, ongoing financial and operational assessments, and alternate communications links. The Commission expects to complete its review of these proposed rules shortly. We also have been working with relevant industry associations – such as the Securities Industry Association and The Bond Market Association – on their members' business continuity and disaster recovery efforts.

Further, the Commission and a number of other financial regulatory agencies (including the Department of the Treasury, Federal Reserve Board, Commodity Futures Trading Commission, Office of Comptroller of the Currency, and Office of Thrift Supervision) participate in the Financial and Banking Information Infrastructure Committee (FBIIC). As you know, FBIIC is designed to coordinate the oversight programs of individual regulators with the President's Critical Infrastructure Protection Board (for potential cyber threats) and the Office of Homeland Security (for potential physical threats). FBIIC initiatives include evaluations of the vulnerability of critical assets for markets and payment systems, improvements in interagency secure communications systems, and the development of protocols for disseminating potential threat alerts from the Office of Homeland Security to regulated entities. In addition, the Commission has joined other FBIIC agencies to ensure that key market participants are able to take advantage of government-sponsored programs designed to facilitate critical telecommunications during emergencies, and to speed the restoration of essential telecommunications lines following a catastrophic outage.

Finally, I should note that the Commission has been working with Federal Emergency Management Agency and New York City and State authorities to improve coordination in the event of future disasters. In particular, we have been focusing on efforts to facilitate the rapid restoration of critical infrastructure services – such as telecommunications, power, water, and transportation – in New York City to key participants in the securities markets following any future catastrophic event in that area.

C. Policy Considerations: Resumption of Clearance and Settlement vs. Resumption of Trading

To date, as the GAO Report correctly indicates, the Commission's intensive efforts have focused on assuring the resilience of the U.S. clearance and settlement system. In our view, the clearance and settlement infrastructure is the single most critical element of the securities markets. As a practical matter, securities transactions cannot be completed in the absence of a functioning clearance and settlement system and, were this system to become incapacitated, the accumulation of failed transactions could create financial exposures in the clearance system and significant systemic risk. This also could make the eventual reopening of the markets all the more difficult. For these reasons, the Commission has given priority to initiatives that assure the prompt implementation of rigorous business continuity plans by these critical entities.

The GAO Report recommends that the Commission do more to assure the resumption of trading by the securities markets and broker-dealers following a major disaster. As noted in the staff's formal comment letter, we share the GAO's views regarding the importance of emergency preparedness of the financial markets, and generally agree with the Report's principle that the financial markets should be prepared to resume trading in a timely, fair and orderly fashion following a catastrophe. By the same token, we also are of the view that individual markets and securities firms are less critical to the securities markets than the key clearance and settlement utilities. For one, trading activity is relatively fungible across markets. In today's diverse U.S. national market system, we find that very few securities are traded only in one market. As a result, we believe that, were any single securities market to become incapacitated, trading could be shifted to one or more of the remaining markets. Of course, sufficient advance preparation is required for any such arrangement to work smoothly and promptly and, as I indicated earlier, Commission staff is in the midst of just such an effort.

As to the resumption of trading by securities firms, in our view, strong business incentives exist for broker-dealers to develop robust business continuity plans for their trading operations. Trading operations, of course, are a source of significant revenue for broker-dealers, and few would risk a situation where their competitors are in a position to trade and they are not. Besides the short-term loss of revenue that would result from this circumstance, there would exist a real possibility of business shifting permanently to more resilient competitors. In addition, customers and counterparties increasingly are seeking assurances that firms have taken appropriate steps to assure their ability to function in the face of even the largest catastrophes.

We also would be concerned with any broad notion that broker-dealers be compelled to resume trading activities. As the staff points out in its comment letter, a broker-dealer's provision of liquidity to the market is voluntary. Because risking capital and providing brokerage services are in essence business decisions, a broker-dealer's choice whether to continue to trade on an ongoing basis or in a crisis is not primarily a matter of government regulation; rather it is governed by the costs involved, relationships with customers, and profitability. Nevertheless, we believe that broker-dealers should

provide customers with access to funds and securities in their accounts as soon as is physically possible, and that business continuity planning expectations must reflect this consideration.

Finally, we note that there are critical policy considerations related to the reopening of the trading markets following a major disaster that could suggest not pursuing the speediest possible recovery. In the event of a disruption of the securities markets, the Commission has a fundamental regulatory interest in assuring the prompt – yet smooth – resumption of trading. Deciding when to reopen the markets will involve an assessment of the operational capabilities of the markets and major market participants, as well as the clearance and settlement system. Difficult judgments may be required to strike the appropriate balance between the desire to resume trading as soon as possible, and the practical necessity of waiting long enough to minimize the risk that, when trading resumes, it will be of inferior quality or interrupted by further problems. For example, in the aftermath of the September 11 events, many praised the decision to wait until Monday, September 17, to reopen the equities markets, as it allowed market participants the preceding weekend to test connectivity and systems, and thereby better assure the smooth resumption of trading.

D. Further Commission Action

Despite these policy considerations, we nevertheless agree with the GAO that more needs to be done to prepare the securities markets for the resumption of trading in the event of a crisis. Specifically, the Commission intends to consider whether it should identify a time frame against which markets should plan to resume trading following a wide-scale regional disaster. By establishing a specific resumption goal, we would provide the securities markets with a consistent benchmark to use in developing more resilient business continuity plans. Such a benchmark could be incorporated into the Commission's existing guidance to markets in this area. That said, we reiterate that, even if the markets are able to resume trading from a technical standpoint, it may not be wise to do so in a given situation if there is significant risk of additional disruptions, or if trading is likely to be of inferior quality. The Commission also intends to continue to work with the New York Stock Exchange, Nasdaq, and the other organized securities markets to develop and test mutual back-up arrangements for various scenarios. Finally, the Commission will work with the markets to increase the resilience of important shared information systems, such as the consolidated market data stream generated for the equity and options markets.

Any timing goal established for the resumption of the trading markets could serve as a useful resumption benchmark for securities firms as well. As previously noted, securities firms have strong business incentives to be prepared to participate in the markets whenever their competitors are in a position to do so. Accordingly, a resumption benchmark for the securities markets may very well act as a *de facto* benchmark for broker-dealers. In addition, the Commission will consider developing standards, in conjunction with the self-regulatory organizations, to help assure that broker-dealers are

able to provide customers prompt access to their funds and securities, even in the face of a wide scale regional disruption.

II. Automation Review Policy (ARP) Program

The GAO Report also recommends that the Commission improve its oversight of operations risk by issuing a rule to require exchanges and clearing organizations to engage in practices consistent with its Automation Review Policy (ARP) program, and by expanding the resources dedicated to the ARP program.

Let me begin by giving you a brief overview of the Commission's ARP program. As a result of our experience during the October 1987 market break and the October 1989 market decline, the Commission issued two Automation Review Policy (ARP) statements regarding the use of technology in the securities markets.² The Commission's Division of Market Regulation established the ARP program to implement the ARP statements. The goal of the ARP statements is to reduce the likelihood that market movements are the result of confusion or panic resulting from operational failure or delays in automated trading and trade dissemination systems. The ARP program implements the ARP statements by assessing the development and management of the automated systems at the exchanges, Nasdaq, clearing organizations, and large electronic communications networks (ECNs). These automated systems are reviewed with respect to capacity, security, systems development methodology, telecommunications, and contingency planning. Commission staff monitor significant interruptions to service in these trading and clearing systems and obtain a periodic update from each organization on present and future developments in their automation systems.

The Commission is dedicated to achieving the goals of the ARP statements. We recognize the critical role that technology plays in the securities industry and, specifically, the importance of having in place adequate safeguards and controls over information resources to ensure reliable and timely trading services to investors.

The events of September 11 underscored the financial markets' critical and increasing dependence on the integrity of their systems infrastructure. The impact of the disaster on market operations confirmed the value of having in place controls over the automated systems that support the U.S. financial markets, including effective contingency plans to facilitate continued trading. In this regard, we share the GAO's views regarding the importance of emergency preparedness of the financial markets.

New technologies that support the financial markets are constantly emerging. The September 11 attacks revealed new market vulnerabilities attributable to catastrophic events that had not been previously contemplated. Similarly, the Commission's approach to reducing the risk of a systems-related market disruption is an evolving one, which must adjust to these developments. In light the GAO's recommendations, we will consider alternative mechanisms to improve the effectiveness of the Commission's

² Securities Exchange Act Release Nos. 27445 (November 16, 1989) [54 Fed. Reg. 48703] (ARP I) and 29185 (May 9, 1991) [56 Fed. Reg. 22490] (ARP II).

automation oversight, including the appropriateness of rulemaking. We also will assess the additional resources that may be necessary to accomplish the objectives reflected in the ARP statements and the GAO Report.

Thank you for the opportunity to testify before you today. I would be happy to answer any questions you may have.

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



February 2003

POTENTIAL TERRORIST ATTACKS

More Actions Needed to Better Prepare Critical Financial Markets


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

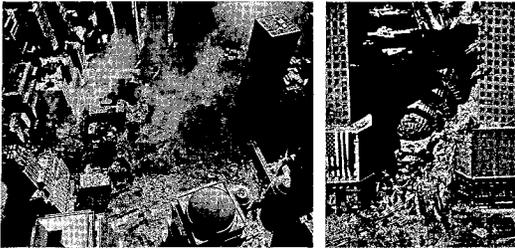
To view the full report, including the scope and methodology, click on the link above. For more information, contact Davi M. D'Agostino (202) 512-8678 or ddago@gao.gov.

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

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

²Board 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

³A 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

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

⁵In 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.

⁶Standards 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.

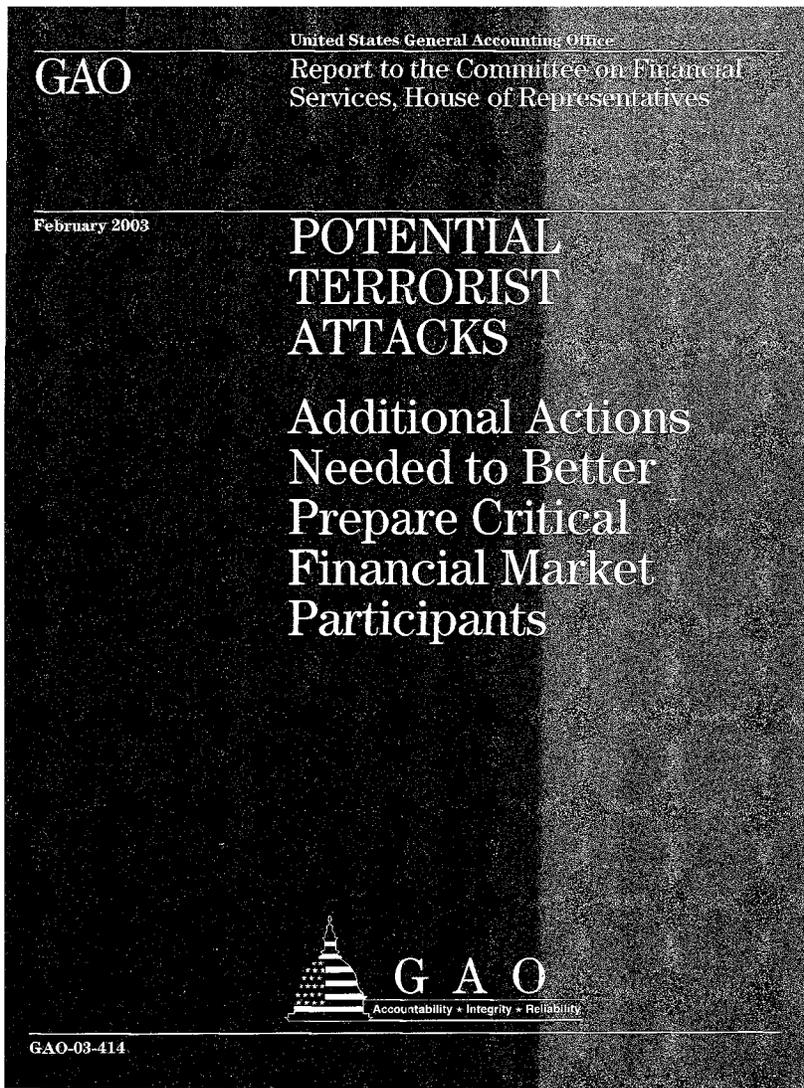
Conclusions

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).



GAO

United States General Accounting Office

Report to the Committee on Financial Services, House of Representatives

February 2003

POTENTIAL TERRORIST ATTACKS

Additional Actions Needed to Better Prepare Critical Financial Market Participants



G A O

Accountability • Integrity • Reliability

GAO-03-414



Highlights of GAO-03-414, a report to the Committee on Financial Services House of Representatives

Why GAO Did This Study

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

What GAO Recommends

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

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

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

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

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

February 2003

POTENTIAL TERRORIST ATTACKS

Additional Actions Needed to Better Prepare Critical Financial Market Participants

What GAO Found

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

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

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



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

Contents

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

Contents

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

 Contents

	Numerous Initiatives Are Under Way to Strengthen the Resiliency of Local Telecommunications Services	100
Appendix III:	Comments from Federal Reserve System	108
Appendix IV:	Comments from the Securities and Exchange Commission	109
Appendix V:	GAO Contacts and Staff Acknowledgments	111
	GAO Contacts	111
	Acknowledgments	111
<hr/>		
Figures	Figure 1: Clearance and Settlement Process for Stocks	20
	Figure 2: Buildings Destroyed or Damaged on September 11, 2001	30
	Figure 3: Geographic Extent of Damage and Debris from Attacks in Lower Manhattan	32
	Figure 4: Damage to Buildings from Attacks and Resulting Debris	33
	Figure 5: Dust and Debris Resulting from Attack	34
	Figure 6: Lower Manhattan Area Subject to Access Restrictions Following September 11, 2001, Attacks	36
	Figure 7: Damage to Verizon Central Office at 140 West Street	38
	Figure 8: Area Served by Verizon 140 West Street Central Office	40
	Figure 9: Verizon Used Temporary Cabling Solutions at 140 West Street	43
	Figure 10: Failed Transactions in the Government Securities Markets During September 2001	50
	Figure 11: Cash Purchases of Government Securities and Repo Market Activity During September 2001	51
	Figure 12: Intervals between Most Recent SEC ARP Examinations of Critical Exchanges and Clearing Organizations	79
	Figure 13: Verizon Overcame Major Challenges During 140 West Street Restoration Efforts	95
	Figure 14: The SFTI Network Provides Redundant Connections	105

Abbreviations

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

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



February 12, 2003

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

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

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

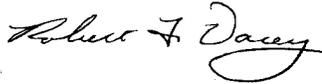
1. the physical and information security and business continuity measures 15 exchanges, clearing organizations, electronic communication networks, and payment system processors had in place after the attacks to reduce the risk of operations disruptions in the future; and
2. the financial regulators'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

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

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



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



Robert F. Dacey
Director, Information Security



Linda Koontz
Director, Information Management



Keith Rhodes
Chief Technologist
Director, Center for Technology
and Engineering

Executive Summary

Purpose

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

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

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

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

Executive Summary

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

Results in Brief

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

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

⁴This guidance included the *Federal Information System Controls Audit Manual, Volume I: Financial Statement Audits* GAO/AIMD-12.19.6 (Washington, D.C.: Jan. 1999); the Federal Financial Institutions Examination Council's *FFIEC Information Systems Handbook: Volume 1*, (Washington, D.C.: 1995); and the Business Continuity Institute's *Business Guide to Continuity Management* (Worcester, United Kingdom: Jan. 19, 2001).

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

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

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

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

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

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

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

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

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

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

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

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

Principal Findings

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Regulators' Oversight of
Operations Risks Had
Limitations

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

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

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

Operations Risks Not Generally Reviewed at Broker-Dealers

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

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

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

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

 Executive Summary

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

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

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

Recommendations

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

**Agency Comments and
GAO Evaluation**

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

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

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

Introduction

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

Various Organizations Participate in Stock and Options Markets

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

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

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

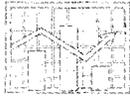
market makers in a particular security by buying and selling shares from their own inventories. Orders for options are often executed on the floors of an exchange in an open-outcry pit in which the representatives of sometimes hundreds of brokers buy and sell options contracts on behalf of their customers.

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

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

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

Figure 1: Clearance and Settlement Process for Stocks

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

Source: GAO analysis of NSCC data.

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

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

Government Securities and Money Market Instruments Are Traded Differently from Stocks

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

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

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

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

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

Payment Systems Processors Transfer Funds for Financial Markets and Other Transactions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Telecommunications and Information Technology Are Vital to Securities Markets

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

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

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

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

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

Objectives, Scope, and Methodology

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

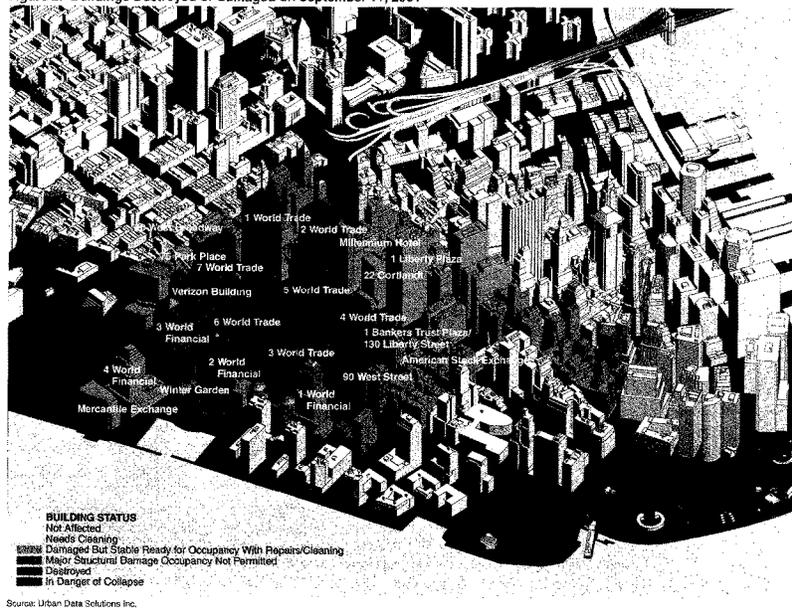
September 11 Attacks Severely Disrupted U.S. Financial Markets

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

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

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

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



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

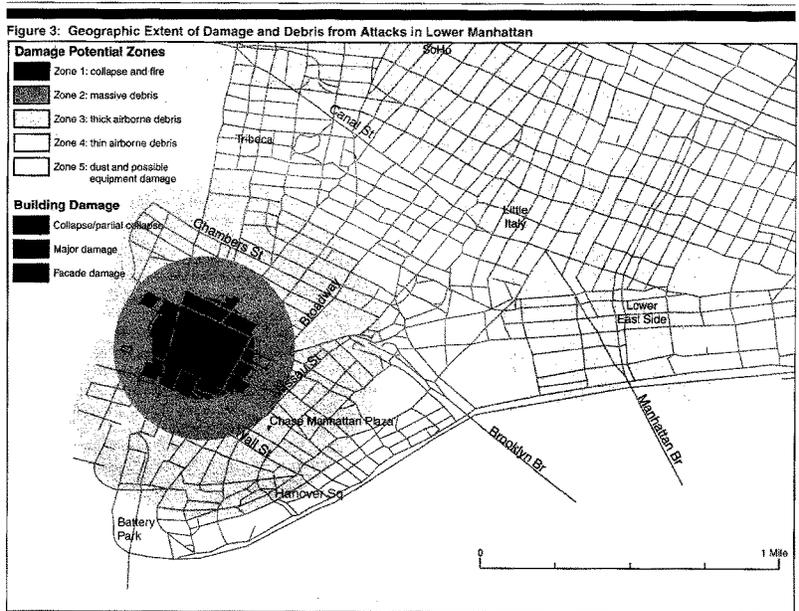
over 13 million square feet of office space, valued at \$5.2 to \$6.7 billion.¹ One of these buildings was 7 World Trade Center, which was a 46-story office building directly to the west of the two towers. It sustained damage as a result of the attacks, burned for several hours, and collapsed around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

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

¹The seventh building was a hotel.

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

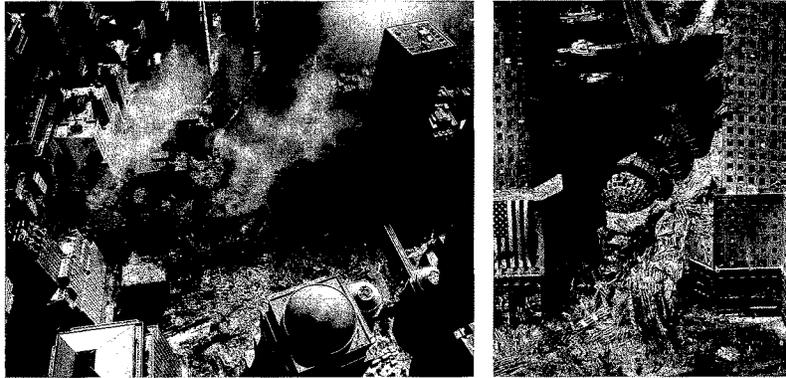
The dust and debris from the attacks and the subsequent collapse of the various World Trade Center structures covered an extensive area of lower Manhattan, up to a mile beyond the center of the attacks, as shown in figure 3.



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

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

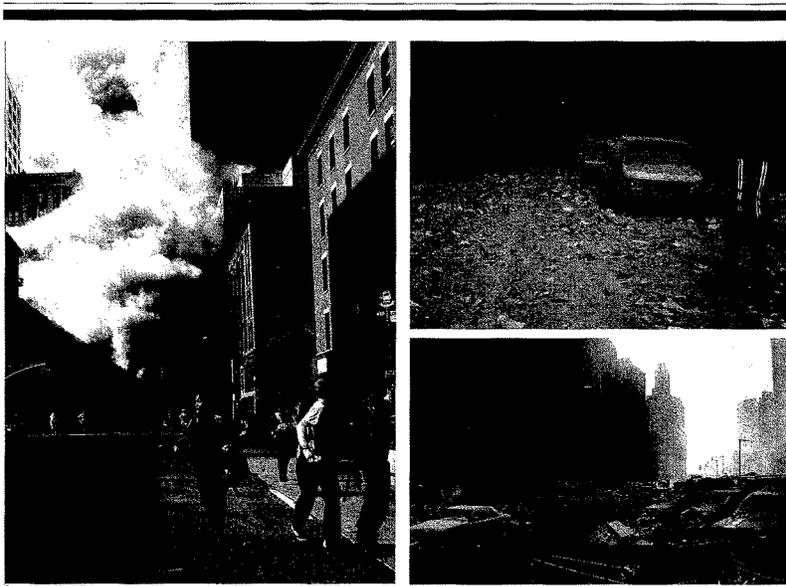
Figure 4: Damage to Buildings from Attacks and Resulting Debris



Source: Associated Press.

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

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



Source: Associated Press.

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

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

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

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

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

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



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

Damage from Attacks Significantly Disrupted Telecommunications and Power

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

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

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



Source: Verizon Communications, Inc.

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

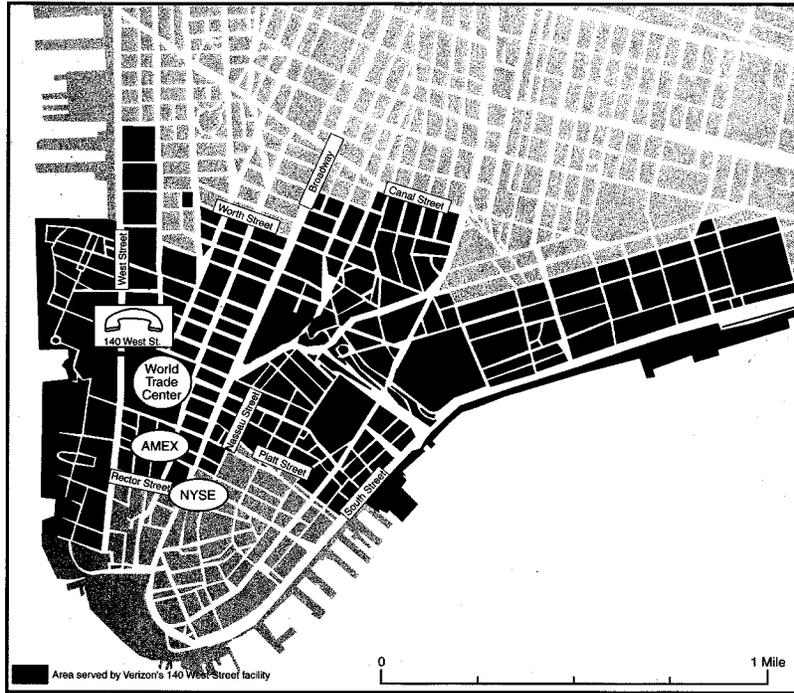
Because of the damage to Verizon facilities and equipment, significant numbers of customers lost telecommunications services for extended periods. When Verizon's 140 West Street central office was damaged, about 182,000 voice circuits, more than 1.6 million data circuits, almost 112,000 private branch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

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

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

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

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



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

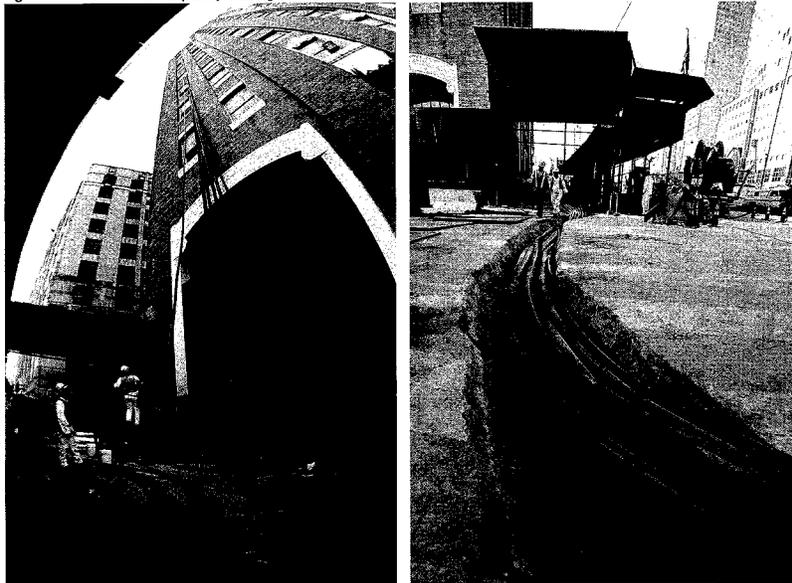
Other telecommunications carriers that serviced customers in the affected area also experienced damage and service disruptions. For example, in 140 West Street, 30 telecommunications providers had equipment that linked their networks to Verizon. Other firms lost even more equipment than Verizon. For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

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

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

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

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



Source: Verizon Communications, Inc.

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

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

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

Most Securities Exchanges and Market Support Organizations Were Not Directly Damaged

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

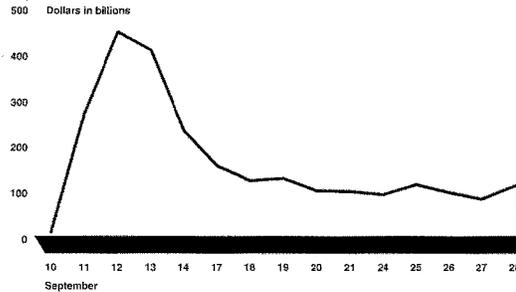
As a result of the attacks, BONY and its customers experienced telecommunications and other problems that contributed to the disruption in the government securities market because it was the clearing bank for many major market participants and because it maintained some of GSCC's settlement accounts.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

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

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

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

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

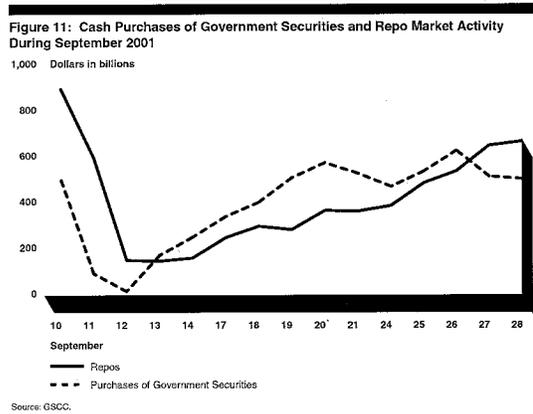


Source: GSCC.

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

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

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



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

The Federal Reserve took several actions to mitigate potential damage to the financial system resulting from liquidity disruptions in these markets. Banking regulatory staff told us that the attacks largely resulted in a funding liquidity problem rather than a solvency crisis for banks. Thus, the challenge they faced was ensuring that banks had adequate funds to meet their financial obligations. The settlement problems also prevented broker-dealers and others from using the repo markets to fund their daily operations. Soon after the attacks, the Federal Reserve announced that it would remain open to help banks meet their liquidity needs. Over the next 4 days, the Federal Reserve provided about \$323 billion to banks through various means to overcome the problems resulting from unsettled government securities trades and financial market dislocations. For example, from September 11 through September 14, the Federal Reserve loaned about \$91 billion to banks through its discount window, in contrast to normal lending levels of about \$100 million.³ It also conducted securities purchase transactions and other open market operations of about \$189 billion to provide needed funds to illiquid institutions. Had these actions not been taken, some firms unable to receive payments may not have had sufficient liquidity to meet their other financial obligations, which could have produced other defaults and magnified the effects of September 11 into a systemic solvency crisis.

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

³The discount window is the lending mechanism used by the Federal Reserve Banks to lend funds to depository institutions on a short-term basis to cover temporary liquidity needs or reserve deficiencies.

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

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

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

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

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

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

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

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

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

Attacks Revealed Limitations in Financial Market Participants' Business Continuity Capabilities

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

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

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

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

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

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

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

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

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

Observations

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

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

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

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

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

Chapter 3
Financial Market Participants Have Taken
Actions to Reduce Risks of Disruption, but
Some Limitations Remain

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

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

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

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

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

Chapter 3
Financial Market Participants Have Taken
Actions to Reduce Risks of Disruption, but
Some Limitations Remain

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chapter 3
Financial Market Participants Have Taken
Actions to Reduce Risks of Disruption, but
Some Limitations Remain

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

Many of the other 8 organizations also had faced increased risk that their operations would be disrupted by wide-scale disasters. At the time we conducted our review, 2 of the 8 organizations had backup facilities that were hundreds of miles from their primary operations. The remaining 6 organizations faced increased risk of being disrupted by a wide-scale disaster because 4 lacked backup facilities, while 2 organizations had backup facilities that were located 4 to 10 miles from their primary operations facilities.³ Of the 4 organizations that lacked a backup facility, one had begun constructing a facility near its primary site.

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

³In total, 4 of the 15 organizations had backup sites 5 miles or less from their primary sites.

Chapter 3
Financial Market Participants Have Taken
Actions to Reduce Risks of Disruption, but
Some Limitations Remain

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

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

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

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

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

Chapter 3
Financial Market Participants Have Taken
Actions to Reduce Risks of Disruption, but
Some Limitations Remain

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

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

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

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

Chapter 3
Financial Market Participants Have Taken
Actions to Reduce Risks of Disruption, but
Some Limitations Remain

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

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

Observations

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Lacking specific requirements under the securities laws, SEC uses a voluntary program to oversee exchange, clearing organization, and ECN information systems operations. U.S. securities laws, rules, and regulations primarily seek to ensure that investors are protected. For example, securities laws require that companies issuing securities disclose material financial information, and SRO rules require broker-dealers to determine the suitability of products before recommending them to their customers. The regulations did not generally contain specific requirements applicable to physical or information system security measures or business continuity capabilities. However, as part of its charge to ensure fair and orderly markets and to address information system and operational problems experienced by some markets during the 1980s, SEC created a voluntary program—ARP—that covered information technology issues at the exchanges, clearing organizations and, eventually, ECNs.⁹ SEC's 1989 ARP statement called for the exchanges and clearing organizations to establish

⁹Initially applied only to exchanges and clearing organizations, SEC extended these ARP guidance expectations under a rule issued in 1998 to any ECN that accounted for more than 20 percent of the trading volume of a particular security; as of September 2002, SEC staff reported that 10 ECNs were subject to all the ARP expectations. Other ECNs must comply with a varying number of the ARP expectations, such as submitting systems change notifications to SEC, depending on their trading volume.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SEC ARP Program Faces
Resource and Staff Limitations

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

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

¹³GAO-01-863.

¹⁴GAO-01-863.

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

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

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

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

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

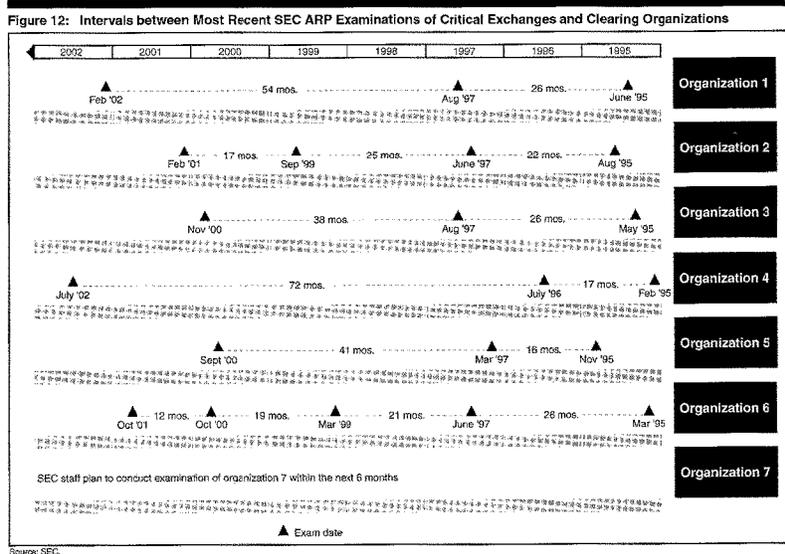
¹⁷Office of Management and Budget, *Appendix III to OMB Circular A-130: Security of Federal Automated Information Resources*.

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

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

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

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



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

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

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

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

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

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

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

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

²¹This \$514 million includes an original appropriation of \$498 million, a \$21 million supplemental appropriation for September 11-related disaster recovery, \$25 million to implement pay parity, and over \$90 million in additional supplemental appropriations.

²²SEC also oversees investment advisers and transfer agents.

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

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

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

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

²³15 U.S.C. §§ 6801, 6805.

²⁴GAO-02-302.

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

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

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

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

Bank Regulators Have Authority to Oversee Operational Risk

As part of their mandate to oversee banks' safety and soundness, the banking regulators, including the Federal Reserve and OCC, issued guidance that directs depository institutions or banks to address potential operations risks with physical and information system security and business continuity measures. The guidance includes recommended steps that banks should take to reduce the risk of operations disruptions from physical or electronic attacks and for recovering from such events with business continuity capabilities. For example, in 1996 these regulators jointly issued a handbook on information systems, which calls for banks to conduct an analysis of their risks and implement measures to reduce them.²⁹ Banks were also to have access controls for their systems and programs. Regarding physical security, the banking regulators expect banks to ensure the safety of assets and to physically protect data centers used for information systems processing. For example, the Federal Reserve's guidance directs banks to take security steps to protect cash and vaults and ensure that bank facilities are protected from theft. The banking regulators' joint 1996 handbook discussed measures to secure data centers and information system assets. However, the bank regulators' guidance did not specifically address measures to protect facilities from terrorist or other physical attacks. Regarding business continuity, the joint handbook expects banks to have plans addressing all critical services and operations necessary to minimize disruptions in service and financial losses and ensure timely resumption of operations in a disaster. Banks also were to identify the critical components of their telecommunications networks and

²⁹Federal Financial Institutions Examination Council, *Information Systems Examination Handbook, Vol. 1* (Washington, D.C.: 1996).

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

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

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

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

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

Conclusions

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

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

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

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

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

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

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

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

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

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

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

Recommendations

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

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

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

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

Agency Comments and Our Evaluation

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

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

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

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

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

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

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

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

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

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

Telecommunications Providers and Others Cooperated to Overcome Damage to Telecommunications Infrastructure

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

The Terrorist Attacks Extensively Damaged Local Telecommunications Infrastructure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Telecommunications
Carriers and
Government Agencies
Worked Together to
Overcome Challenges**

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

**Telecommunications
Carriers Gave First Priority
to Government and Health
Care Services**

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

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

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

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

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

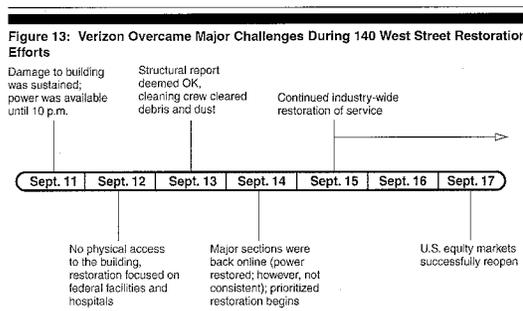
Telecommunications
Companies Overcame
Numerous Restoration
Challenges

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

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

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

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



Source: Verizon Communications, Inc.

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

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

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

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

City Officials Helped
Coordinate Carrier
Restoration Efforts

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

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

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

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

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

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

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

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

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

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

**Regulators and Market
Participants Are Acting
to Improve Crisis
Response**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

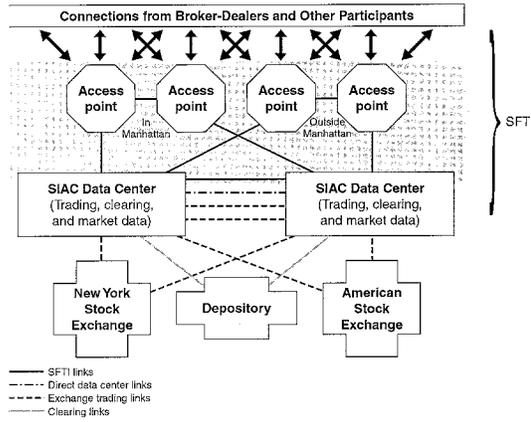
region causing disruption to supporting infrastructure (e.g., telecommunications and electrical power). In phase 1 tests, participants are required to test communications facilities between their own backup sites and the primary sites of critical parties. During phase 2 testing, all test participants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

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

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

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

Figure 14: The SFTI Network Provides Redundant Connections



Source: Securities Industry Automation Corporation.

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

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

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

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

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

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

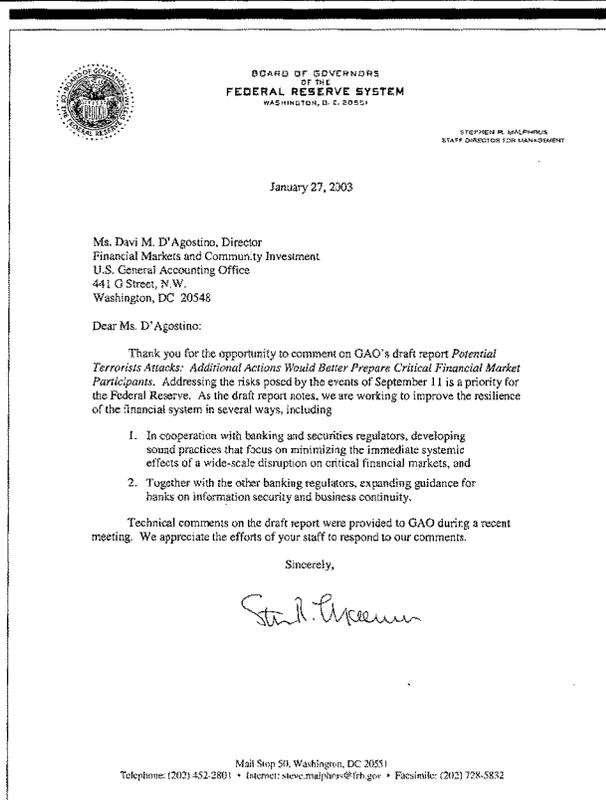
⁷Con Edison Communications, a wholly owned subsidiary of Consolidated Edison, Inc., builds and operates its own fiber-optic network providing data communications services and custom network solutions to multiple classes of customers, including telecommunications carriers, corporations, and Internet,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

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

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

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

 Comments from Federal Reserve System



Appendix IV

Comments from the Securities and Exchange Commission

 DIVISION OF MARKET REGULATION	UNITED STATES SECURITIES AND EXCHANGE COMMISSION WASHINGTON D.C. 20549
	January 21, 2003
<p>Ms. Davi M. D'Agostino Director, Financial Markets and Community Investment United States General Accounting Office 441 G Street, N.W. Washington, D.C. 20548</p>	
<p>Dear Ms. D'Agostino:</p> <p>This letter responds to your request to review and comment on the draft report entitled <u>Potential Terrorist Attacks: Additional Actions Would Better Prepare Critical Financial Market Participants</u>, GAO-03-251. We appreciated the opportunity to meet with you and your colleagues to convey comments on the report and appreciate your willingness to address our comments in your report.</p> <p>We share the GAO's views regarding the importance of emergency preparedness of the financial markets. As the report recognizes, we have been working actively with the trading markets and the major market participants to strengthen their resiliency. Accordingly, we generally agree with the report's principle that the financial markets should be prepared to resume trading in a timely, fair and orderly fashion following a catastrophe.</p> <p>As we indicated in our meeting with you and your colleagues, we have some concerns with the recommendation that we ensure that broker-dealers implement sound business continuity practices to resume trading. Specifically, it should be recognized that a broker-dealer's provision of liquidity to the market is voluntary. Because risking capital and providing brokerage services are in essence business decisions, a broker-dealer's choice whether to continue to trade on an ongoing basis or in a crisis is not primarily a matter of government regulation; rather, it is governed by the costs involved, relationships with customers, and profitability. In contrast, when a significant trading market or broker-dealer has executed trades, it must process these outstanding trades promptly, in order to reduce financial exposures in the clearance system and reduce systemic risk. Similarly, broker-dealers should provide customers with access to funds and securities in their accounts as soon as is physically possible. We believe that business continuity planning expectations must reflect these various considerations.</p> <p>With respect to the Commission's Automation Review Policy ("ARP") program, we agree with the GAO's recognition of the importance of market participants appropriately responding to ARP recommendations. As the Commission stated in ARP</p>	

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

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

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

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

Sincerely,



Annette L. Nazareth
Director

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

GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Acknowledgments

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

GAO's Mission

The General Accounting Office, the 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs**Contact:**

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

Public Affairs

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

1399 New York Avenue, NW
Washington, DC 20005-4711
Telephone 202.434.8400
Fax 202.434.8456
www.bondmarkets.com

360 Madison Avenue
New York, NY 10017-7111
Telephone 646.637.9200
Fax 646.637.9126

St. Michael's House
1 George Yard
London EC3V 9DH
Telephone 44.20.77 43 93 00
Fax 44.20.77 43 93 01



***Testimony of Micah S. Green
President, The Bond Market Association***

***Before the
United States House of Representatives
Committee on Financial Services Subcommittee on Capital Markets***

***Hearing on the General Accounting Office Report on Recovery and
Renewal Efforts Post Sept. 11
February 12, 2003***

I would like to thank Chairman Oxley and Chairman Baker for the opportunity to testify today on The Bond Market Association's efforts to help restore trading in the bond market following the attacks of September 11, 2001 and steps we have taken to prepare for emergencies in the future. I am Micah S. Green, president of The Bond Market Association, which represents approximately 200 securities firms and banks that underwrite, trade, and sell fixed-income securities both domestically and internationally.

The despicable attacks on America in September 2001 wrought tragic consequences for thousands of New Yorkers and Washingtonians. Indeed, no American has been untouched by those events. The financial services industry was especially affected by the attacks. A significant portion of the 2,800 people killed in the attacks made their living in the capital markets, and a large number of them worked in the bond markets. It was a tragic time that tested the mettle of the families, friends and colleagues of those who were killed. At the same time, September 11 elicited noble actions on the part of many, including many fixed-income market professionals.

The Bond Market

Many people do not realize that the U.S. bond markets dwarf the stock markets in size, with respect to both outstanding securities and volume of transactions. Through the third quarter of 2002, there were nearly \$20 trillion of bonds and other fixed-income securities outstanding versus a total stock market capitalization of \$11.5 trillion. Average daily bond market "cash" trading volume in the first half of this year was nearly \$630 billion, compared to a \$64 billion combined average volume on the three major stock markets. Hundreds of billions of dollars more in transactions are conducted daily under repurchase agreements. Processing such a large volume of fixed-income transactions every day requires a highly sophisticated and automated market infrastructure composed of numerous players. These participants are all inter-connected via complex telecommunications links. Also, unlike a stock market such as the New York Stock

Exchange, bonds trade in a decentralized, over-the-counter market. There is no single, central physical point of contact for participants in the bond markets, save, perhaps, for certain clearance and settlement facilities.



There is, of course, a concentration of financial services firms in lower Manhattan. Several key participants in the U.S. fixed-income markets were located in or near the World Trade Center. Both Cantor Fitzgerald and Garban/ICAP, two of the largest fixed-income inter-dealer brokers, had their principal New York offices in the twin towers. Morgan Stanley, one of the largest participants in the fixed-income markets, was also one of the Trade Center's largest tenants. Two more of the market's largest fixed-income dealers, Merrill Lynch and Lehman Brothers, were located in the World Financial Center, which, of course, sustained significant physical damage. Euro Brokers, another fixed-income inter-dealer broker, also had its offices in the World Trade Center. The market's two largest clearing banks, the Bank of New York and J.P. Morgan Chase—together responsible for processing hundreds of billions of dollars in transactions every day—were located just a few blocks from ground zero. Numerous other firms active in the markets had offices in or near the World Trade Center and were directly affected by the attacks. The Bond Market Association itself was displaced from its New York offices on Broad Street in lower Manhattan for a week after September 11.

The Association plays an important role in market operations by bringing together dealers and other participants and fostering open discussion of critical issues. In addition, the Association helps facilitate orderly and efficient markets by issuing market practice recommendations to dealers. These recommendations generally cover areas such as clearance and settlement, documentation and standard calculations. Compliance is purely voluntary. The Association's role as a forum for discussion and issuer of market practice recommendations help ensure that the markets operate smoothly. This was never more important than in the days following the terrorist attacks.

A Speedy Resumption of Bond Trading Following the Attacks

On the morning of September 11, the staff of the Association, along with most others in lower Manhattan, evacuated its offices when the planes crashed into the World Trade Center and the twin towers fell. Later that day, after consulting with key market participants and regulators, Association staff issued a recommendation that the U.S. fixed-income markets be closed until further notice.¹ Again, compliance with the Association's recommendations is strictly voluntary. In reality, the decentralized, over-the-counter fixed-income markets never close. Participants are free to trade with each other any time they wish. Moreover, the fixed-income market, especially the market for U.S. government securities, is truly global in nature. Government securities trading takes place in every major financial center in the world. Our recommendation for a market close on September 11 and 12 applied only to New York trading hours.

¹ A detailed account of emergency meetings and actions taken by the Association following the attacks on September 11 is available on the Association's Web site at www.bondmarkets.com/market/9-11_minutes.shtml.



On September 12, we convened several conference calls with Association leadership and government officials to determine whether market participants felt prepared to resume activity on September 13. It quickly became clear that the fixed-income markets had suffered extraordinarily on September 11. Both Cantor Fitzgerald and Euro Brokers, important sources of market liquidity, were tragically devastated. Garban/ICAP, another important source of liquidity, lost its primary trading facility. (Fortunately, Cantor's backup facility in New Jersey and its London location were soon able to support trading via their electronic trading platform, eSpeed.) The two major clearing banks that support the system for clearing and settling securities transactions had lost significant telecommunications capability. A number of dealers did not have access to their primary trading sites in lower Manhattan. Personnel were strained by dealing with issues and problems raised by the attacks, often in backup facilities. Nevertheless, the consensus of our membership was that, despite the extreme loss of life and other hardships, the market was ready to resume activity on September 13. We issued a statement on the afternoon of September 12 recommending that the market reopen, albeit with an abbreviated trading day and an extended cycle for clearing and settling trades in government securities. On the morning of September 13, less than 48 hours after the first plane was flown into the World Trade Center, the bond markets resumed trading.

The trading day on September 13 proceeded fairly smoothly in an abbreviated session. The biggest problem the market faced was clearing and settling transactions from previous trading days. Since the bulk of government securities cash and repo trading takes place before 9:00 a.m., it is important to note that September 11 was close to a full trading day. Telecommunications connectivity problems among the largest dealers, the Government Securities Clearance Corporation (GSCC) and the two largest clearing banks led to the inability of these institutions to reconcile their systems due to incomplete trade and settlement information. Over the next several days, the Association hosted a number of conference calls with key market participants and regulators to address the problem. Although some market participants continued to experience problems in the area of clearance and settlement, the markets slowly returned to normalcy in the weeks following the attacks.

Because of the disruption to normal clearance and settlement activities that resulted from the attacks, the Association, in consultation with regulatory authorities, also considered whether to issue recommendations that market participants allow extended settlement terms on a temporary basis. Transactions in government securities and bonds issued by government-sponsored agencies typically settle the day after the transaction is executed—so-called "T+1" settlement. In order to ensure that market participants who may have lost telecommunications connectivity to clearing banks and clearance and settlement utilities had adequate time to process transactions, we recommended an extended settlement cycle for government and agency securities—first to the third day after trade execution, or T+3, and then to T+5—in the days following September 11. We also continued to recommend abbreviated trading hours, with early market closes of 2:00 p.m. We believe these actions helped some market participants deal with telecommunications systems destroyed in the attacks. By September 20, most systems had been brought fully back online, and we had withdrawn our recommendation for

4

abbreviated trading hours. By Monday, September 24, we had withdrawn our recommendation for extended settlement cycles.



The Association helped the recovery in other ways, as well. Our Manhattan office of the Association was inaccessible during the week following the attacks and suffered spotty telephone and data communications even after we returned. During that time, our Washington and London offices coordinated communications among industry members and with government officials. We also helped industry members with facilities located in lower Manhattan work with federal and city agencies to gain access to their buildings when that part of the city was effectively shut down. This helped market liquidity in the days following the attacks by ensuring that dealers who wanted to trade were able to do so.

The quick recovery of the bond markets following such a destructive attack is a testament to the thousands of dedicated fixed-income professionals who worked very hard under extremely difficult conditions in the days following September 11 to bring the markets back. It is also a demonstration of the resiliency of decentralized, over-the-counter market, which are not dependent on a single physical location in order to continue trading in the face of a market emergency.

Lessons of 9/11: Business Continuity Planning

The market continues to learn from the experiences of September 11. Contingency planning has become more than just a new buzzword. Virtually every major market participant has now developed and implemented plans for dealing with disasters of the scale we witnessed in 2001. The Association has implemented its own contingency planning. In the event of another emergency of the scale and impact of September 11, Association leadership, staff and members of key committees will meet via conference call to assess the situation and make recommendations on market operations.

The Association has also worked closely with other industry groups, including the Securities Industry Association (SIA), whose representative is also testifying here today, to help ensure that market participants and government officials are able to make contact with each other and coordinate responses should a major disaster occur again.

Regulators have also examined issues raised by September 11 attacks. In May 2002, the Federal Reserve Board (Fed) and the Securities and Exchange Commission (SEC) issued a white paper outlining issues raised by September 11 with regard to the nation's clearance and settlement systems for government securities. In particular, the two agencies asked whether the clearance and settlement system for government securities is too concentrated and whether changes are warranted. The Association told regulators that the current clearance and settlement system has evolved as a result of market forces. The Association told the Fed and the SEC that although wholesale, mandated changes are not warranted, certain steps to mitigate systemic risks are worth considering. (Please see appendix A for a copy of the Association's comment letter on this issue.)



In addition, in August of last year, the SEC, Fed, and Office of the Comptroller of the Currency issued a draft white paper discussing business contingency steps that clearing organizations and other firms that play significant roles in critical financial markets would be expected to implement. The Association submitted a joint comment letter with the SIA which supported continuing efforts to fortify contingency plans and systems but argued against imposing inflexible “one-size fits all” requirements on each firm. The agencies have been considering these and other comments in preparation for issuing a final white paper. (Please see appendix B for a copy of the Association’s joint comment letter with the SIA on this issue.)

The Association has established the Business Continuity Management Council (BCMC) to engage members in fixed-income-specific business continuity issues. The BCMC is made up of senior fixed-income operations and business continuity professionals from the Association’s member firms and works closely with the SIA’s Business Continuity Planning Committee. The Association also works with the SIA and the American Bankers Association on business continuity issues through the Federal Financial Services Sector Coordinating Council (FSSCC). The FSSCC is an industry organization that coordinates with federal financial services regulators on security issues.

The Association and the SIA have also been working with various telecommunications industry associations and federal committees to encourage dialog with industry leaders, the FCC and others to achieve real change in the telecommunications infrastructure. Resilience in telecommunications, which is the bedrock of the bond market, should support resilience in bond market operations infrastructure. This support would enable us to trade more effectively in the event of another business disruption.

MSRB Trading Halt Proposal

In the aftermath of September 11, federal regulators and self-regulatory organizations have been appropriately focused on whether they have the authority and means necessary to address market emergencies. As an outgrowth of this review, the Municipal Securities Rulemaking Board (MSRB) recently filed a rule proposal seeking the authority to declare an emergency halt to trading in the municipal securities market. At the SEC’s request, the MSRB recently extended by 30 days what was to have been an unusually brief comment period. The Association is grateful to have the opportunity for a more thorough vetting of the important policy implications presented by the MSRB’s proposal.

While the Association appreciates the MSRB is motivated by the need to address issues raised by the tragic events of September 11, we believe that the case has not been made for new trading halt authority, and that imposing a blanket trading halt on the entire municipal bond market is on balance likely to do more harm than good. Even in times of stress or damage to “critical infrastructure,” bond market participants should be permitted to trade and to provide liquidity to investors and each other that is critical to our nation’s economy and banking system. Rather than focus on closing the market, the aim should be to prepare for keeping the market open in times of emergency.



The fixed-income markets are inter-linked, global and trade continuously and are highly inter-related. Accordingly, any consideration of whether to grant trading halt authority in the municipal markets should be undertaken only in conjunction with a broader review of how a market emergency may impact fixed income markets generally. The decision to suspend trading in a specific security should not be made without consideration of the effect it will have on the market for other fixed-income securities. It follows that the authority to suspend trading in a specific security, if deemed necessary, should not rest with a non-governmental agency with a limited mandate.

The Association strongly believes that the focus of debate concerning the proposal should be on the significant public policy issues surrounding the appropriateness of a trading halt in an OTC market, and ultimately on what is in the best interest of the investing public and the nation's economic and financial system. Every other question is secondary. The Association's concerns—briefly outlined below—were discussed in a letter to the President's Working Group on Financial Markets (see appendix C) and will be detailed in a more comprehensive comment letter to be filed with the SEC.

▪ **A Blanket Trading Halt Is Unlikely To Be Needed, Or Helpful**

Because the OTC bond markets are decentralized and flexible, there is no need for a blanket trading halt. The proposed “cure” of closing the market in times of emergency likely would do more harm than allowing the private sector to function and adapt to the circumstances.

Because there is no exchange or central platform needed for trading fixed-income securities, trading can occur on a bilateral basis even in times of disruption so long as individual parties have the capacity to do so. The only possible central point of failure is the settlement and clearance system provided by the Depository Trust and Clearing Corporation (“DTCC”). But even if DTCC—which has its own sophisticated contingency plans in place—were to encounter difficulties, parties can decide whether to refrain from trading, or to extend the settlement period, or to make alternate settlement arrangements. Hence, even during an emergency, private sector participants should have the flexibility to decide whether to trade, subject to investor protection rules.

Moreover, the municipal securities market, to which the MSRB's proposal would apply, is actually the smallest sector of the U.S. bond market in terms of trading volume. Less than two percent of total daily bond market trading volume is in municipals. In the days following September 11, municipal market volume actually fell significantly. Even if there was a significant breakdown in the nation's clearance and settlement system, the low transaction volume in the municipal sector suggests it would be least affected. The low volume also suggests that alternative clearance and settlement arrangements would potentially be viable.

Whatever the circumstances, there is a benefit to economic and banking policy makers in allowing market participants to express views on credit and rates in a continuous way and

7

to provide liquidity for investors who need it. The Association's members are major participants and providers of liquidity in the municipal bond market and the other OTC bond markets. Their own knowledge and experience informs their strong belief that the flexibility to continue trading and to provide liquidity would in all conceivable circumstances be better than a regulatory market close.



▪ **September 11 Demonstrated The Market's Resilience**

The performance of the fixed income markets following September 11—as detailed above—helps illustrate why a blanket trading halt is unlikely to be necessary or helpful. Market participants were able to communicate and make voluntary adjustments to respond to the circumstances. Regulators and market participants recognized the importance of re-opening the markets quickly, to restore the financial markets and to support national security and confidence.

It also bears noting that the difficulties encountered with the clearance and settlement of Treasury securities following September 11 related almost entirely to trades executed *before* the terrorist attacks on September 11. A trading halt issued after the crisis occurred, such as the MSRB contemplates in its proposal, would not have avoided these problems.

▪ **Targeted Rules And Procedures Are Preferable To A Market Close**

Rather than focus on closing the markets in an emergency, it would be better to work toward keeping the markets open. This can be achieved by targeting issues that might arise during an emergency with firm-specific measures and enhanced investor protection and capital adequacy rules. Moreover, to the extent the MSRB is motivated by a concern that market participants could take advantage of a chaotic market to commit fraud or abuse, it should be noted that investor protection and anti-fraud rules are already in place.

The Association recognizes that the worthy goal of the MSRB and other regulators is to prepare for emergencies such as September 11. But we believe it would be better to work toward keeping the markets *open* in such circumstances, rather than focus on *closing* the markets. As noted above, the Association is currently working with other industry groups and federal financial regulators on business continuity plans intended to minimize the disruption to the financial system in the event of an emergency. Ironically, because firms devote resources to business continuity measures partly to be able to continue trading when other firms are unable to, the ability to halt trading by all firms could act as a disincentive to strengthen such measures.

Conclusions

The terrorist attacks of September 11, 2001 sent an emotional and physical shock through the bond market, tearing apart lives along with the market infrastructure. Despite countless personal tragedies, bond market participants—with the Association acting as a facilitator and in consultation with regulators—rallied to reopen trading in only two days.

8

The display of resolve is testament to the dedicated professionals in our industry who immediately grasped the broader importance of returning the financial markets to normalcy as quickly as possible.



September 11 also serves as a valuable reminder of the need to always be prepared. Though bonds are traded in a decentralized, over-the-counter fashion, the Association and its members recognize the value of business continuity planning to minimize the disruptions stemming from any future emergencies. The Association is working with other sectors of the financial industry and regulators on this issue. While guidance and new rules in this area governing critical market infrastructure may be necessary, the Association opposes the MSRB's proposal to adopt the authority to suspend trading in the municipal bond market. Regulatory efforts should remain focused on keeping the markets open in times of crisis, not on the authority to close markets.

Appendix A

40 Broad Street
New York, NY 10004-2373
Telephone 212.440.9400
Fax 212.440.5260
www.bondmarkets.com

1399 New York Avenue, NW
Washington, DC 20005-4711
Telephone 202.434.8400
Fax 202.434.8456

St. Michael's House
1 George Yard
London EC3V 9DH England
Telephone 44.20.77 43 93 00
Fax 44.20.77 43 93 01



August 19, 2002

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the
Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, D.C. 20551

Mr. Jonathan G. Katz
Secretary
Securities and Exchange Commission
450 5th Street, NW
Washington, D.C. 20549

RE: Docket No. R-1122, Interagency White Paper on Structural Change in the Settlement of Government Securities: Issues and Options

Dear Ms. Johnson and Mr. Katz:

The Bond Market Association ("we" or the "Association"¹) appreciates the opportunity to comment on the White Paper entitled "Structural Change in the Settlement of Government Securities: Issues and Options" (the "White Paper"), jointly issued by the Federal Reserve Board (the "Board"), and the Securities and Exchange Commission (the "Commission", collectively with the Board, the "Agencies") in May 2002. The Association applauds the Agencies for their examination of issues related to the clearance and settlement of U.S. government securities.² We believe that, given the important role the clearance and settlement system plays in the government securities markets, an examination of the issues related to the clearance and settlement system is a worthwhile and necessary exercise.³

Given the length of our letter, and in order to facilitate your review and easy reference, below please find a table of contents.

¹ The Association represents securities firms and banks that underwrite, distribute and trade in fixed income securities, both domestically and internationally, including all primary dealers recognized by the Federal Reserve Bank of New York. Our members are also actively involved in the funding markets for such securities, including the repurchase and securities lending markets. This letter has been the subject of intensive and widespread discussion within our membership and was drafted based on the input of the Association's Board and the following Association committees: Interagency White Paper Response Task Force, Primary Dealers Executive Committee, Primary Dealers Committee, Funding Division Executive Committee, Government Operations Committee, Risk Management Steering Committee, MBS Operations Committee, Government Legal Advisory Committee and the Funding Division Legal Advisory Committee. Further information regarding the Association and its members and activities can be obtained from our web site www.bondmarkets.com.

² For purposes of this letter, we use the term "government security" to refer to securities that are eligible for the Fedwire book entry system.

³ In fact, the European Union ("EU") and the European Parliament are also currently in the process of evaluating how to create a more stable, efficient and integrated clearance and settlement system for Europe. A report recently published by the Commission of the European Communities focuses heavily on the importance of a well-functioning clearance and settlement system for facilitating the growth of a deep, liquid, efficient and cost-effective financial market. See Commission of the European Communities: Communication from the Commission to the Council and the European Parliament entitled "Clearing and Settlement in the European Union, Main Policy Issues and Future Challenges," (Brussels, May 28, 2002).

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY3
 1.1 Central Observations3
 1.2 Advisory Committee.....4
 1.3 Adequacy Of The Current Government Securities Clearance System.....5
 1.4 Private Limited Purpose Bank5
 1.5 Old Euroclear Model6
 1.6 Enhancement Of Federal Reserve Services7
 2. BACKGROUND.....7
 3. METHODOLOGY FOR THE EXAMINATION OF A GOVERNMENT SECURITIES CLEARANCE AND SETTLEMENT SYSTEM10
 3.1 Sufficient funds and securities must be available to market-makers, not only in "normal" market conditions, but also in times of market stress, to support a deep, liquid and transparent trading market.10
 3.2 Operational and exit risks that could disrupt the clearance and settlement process must be adequately mitigated.....13
 3.3 Incentives should exist for service providers to pursue innovations and invest in research and development (resulting from technology advances or trading practice advances) that are necessary to respond to the needs of market participants.....14
 3.4 The costs of operating the clearance and settlement system (including conversion costs associated with alternative or structural changes) should be reasonable and efficiently borne relative to the benefits afforded market participants.....15
 4. ENHANCING THE CURRENT SYSTEM.....17
 4.1 The current government clearance and settlement system allows for a high level of liquidity in the government securities markets by providing an adequate amount of intraday financing to dealers.....17
 4.2 The current government securities clearance and settlement system presents a level of operational and exit risk that can be managed within the existing system17
 4.3 Creation of a data and software repository may also alleviate problems arising from the exit of a clearing bank, while maintaining the level of intraday liquidity under the current system.....18
 5. CONCLUSION19

Appendix A - Analysis of the Current Government Securities Clearance System

Appendix B - Analysis of the Limited Purpose Bank Approach

Appendix C - Analysis of the Old Euroclear Model

Appendix D - Analysis of Enhancing the Federal Reserve System

Appendix E - List of Task Force Members

1. EXECUTIVE SUMMARY

1.1 Central Observations

The Association *believes that*:

- The most important element of any government securities clearance and settlement system is the ability of such system to provide adequate intraday financing to dealers to maintain and enhance the high level of liquidity that the government securities trading and funding markets currently enjoy.
- The prudent availability and access to cash and securities currently provided by JP Morgan Chase ("Chase") and the Bank of New York ("BONY", collectively with Chase, the "Clearing Banks") is crucial to the proper functioning of the government securities markets and the critical role these markets play in the global economy, as both a credit risk-free price discovery benchmark and a vehicle for financing the Federal government's operations.
- While it is difficult to predict whether an alternative structure may successfully separate "core" clearance and settlement from triparty repo services, our initial view is that such services would be difficult to unbundle.
- The current "duopoly" for the provision of clearance and settlement services is the result of natural market forces and therefore should not be artificially restructured, especially with the limited resources currently available to many dealers to explore different alternatives.
- While the "exit risk" connected with the Clearing Banks is indeed a real risk which is of appropriate concern to policy makers, the Association believes it is somewhat overstated in the White Paper and can be mitigated within the context of the existing structure.
- The majority of governmental and industry resources should be devoted to examining the manner in which risks in the current government securities clearance system can be addressed within the current structure, at least in the short-term.
- The development of common communications protocols, and the creation of a real-time data and software backup repository jointly shared by the Clearing Banks are potential enhancements to the existing system that should be explored as soon as possible.
- Alternative approaches that are not identified in the White Paper should also be considered.

1.2 Advisory Committee

The Association respectfully urges the formation of a Government Securities Clearance System Advisory Committee (the "Advisory Committee"). Such committee should be organized under the auspices of one or both of the Agencies, or pursuant to the Federal Advisory Committee Act.⁴ The mission of the Advisory Committee would be not only to explore the viability of the alternative structures outlined in the White Paper, but also to consider enhancements to backup/contingency arrangements and to serve as a vehicle for coordinated actions in the event of a voluntary or involuntary exit of one of the Clearing Banks or other dislocations.⁵ The formation of an Advisory Committee will also permit a level of open dialogue regarding competitive issues that a purely "private" group might be legally or commercially inhibited from discussing.⁶

We recommend that the Advisory Committee be composed of representatives from the Clearing Banks; the Depository Trust and Clearing Corporation ("DTCC", including representatives from the Government Securities Clearance Corporation (GSCC) and the MBS Clearing Corporation (MBSCC)); custodian banks; and representatives from relevant trade associations, the primary dealers⁷ and institutional investors. This Advisory Committee should work with representatives from the Agencies, as well as with the Federal Reserve Bank of New York ("FRBNY") and the U.S. Department of the Treasury ("Treasury"), to more closely examine the issues raised by the White Paper, and to recommend and pursue as soon as practicable concrete steps to address such issues.⁸

⁴ Pub. L. 92-463, Oct. 6, 1972, 86 Stat. 770. One alternative that may be worth exploring is having the Federal Reserve sponsor the Advisory Committee. The Federal Advisory Committee Act ("Advisory Committee Act") imposes certain procedural and record-keeping requirements that may reduce the effectiveness of the Advisory Committee. However, these technical requirements do not apply to certain committees including advisory committees established or utilized by the Federal Reserve System. See Advisory Committee Act, Section 4(b).

⁵ For example, one of the functions of the Advisory Committee would be to coordinate Clearing Bank disaster recovery planning and facilitate industry-wide scenario-based contingency planning and testing.

⁶ In general, coordinated commercial responses within an industry can raise serious issues under U.S. antitrust law that need to initially be addressed in order for adequate contingency planning and testing to be undertaken on an industry-wide basis. We believe the Advisory Committee, because of government participation, is an appropriate venue for open dialogue on these issues between and among competitors. See, e.g. *Parker v. Brown* 317 U.S. 341 (1943) (conduct among competitors that is undertaken at the direction of government may enjoy limited protection from antitrust law); see also The Bond Market Association's Antitrust Guidelines (July 1998) available at www.bondmarkets.com.

⁷ As noted in Appendix A to the White Paper, the trading of U.S. government securities, including federal agency securities and mortgage-backed securities is concentrated largely among the 22 primary dealers. Throughout the Association's response, the use of the word "dealer" or "primary dealer" is intended to refer to the 22 primary dealers through which the majority of trading volume in U.S. government securities takes place.

⁸ We do not believe that the Advisory Committee should have any independent regulatory authority, and we are not recommending any specific statutory changes to the existing federal regulatory regime for this market. As noted above, the purpose of the Advisory Committee is simply to facilitate further examination of the issues raised by the White Paper, and, if appropriate, publicly recommend steps to address such issues. Needless to say, any conclusions of the Advisory Committee with respect to any improvements to or restructuring of the current system should serve as a guide to - and not a substitute for - natural market forces.

1.3 Adequacy of the Current Government Securities Clearance System

As explained in further detail in Appendix A, the Association believes that the current clearance and settlement system provides a stable and efficient structure for the clearance and settlement of government securities. In particular, the current system provides liquidity crucial to the government securities market by providing adequate amounts of intraday financing to the dealer community. While risks exist in the current system, the Association believes that ongoing and future initiatives could adequately address such risks while maintaining the current system's existing structure. *As discussed in detail below, given the conversion costs of restructuring the current system, and given the uncertainty associated with the ability of an alternative system to support a deep and liquid government securities market, the Association recommends that the majority of the industry's and the regulatory community's efforts should be initially focused on enhancing the present system, at least in the short term.* However, the Association also believes that as part of a longer term strategy, the industry should explore in more detail alternative clearance and settlement structures, including certain of the alternatives outlined in the White Paper.

With respect to the current government securities clearance system, the Association *notes that:*

- The risks inherent in the current clearance and settlement system for government securities should, in the short term, be addressed within the current system.
- The voluntary exit risk present in the current system should be mitigated through private bilateral commercial assurances and express commitments by the Clearing Banks to regulatory authorities that they will not exit the clearing business without adequate notice.
- Problems arising through the involuntary exit by a Clearing Bank resulting from a criminal indictment or guilty plea, criminal conviction, or receivership or other financial difficulties be mitigated through the immediate development of an orderly transfer or unwind plan.
- The possibility of creating a common data and software repository for both Clearing Banks be further examined to determine the feasibility of this approach and the costs associated with its implementation.
- Operational risk be further mitigated through the continued development of robust contingency and back-up arrangements by key service providers and protocol initiatives that promote technological/systems interoperability between the Clearing Banks.

1.4 Private Limited Purpose Bank

The Association believes that this approach presents a number of potential benefits, including mitigating certain of the exit risks present in the current system. As discussed in Appendix B, this alternative would involve the formation of a single industry-owned private limited purpose bank (the "LP Bank") that was a member of the Federal Reserve System that would provide core clearance and settlement services, and potentially other services such as triparty repo services. The Association has some concerns about this approach, including

the ability of the LP Bank to provide adequate intraday financing and securities lending to the government securities markets. While such concerns remain, the Association believes that these concerns might be overcome and that the potential benefits of this approach justify a closer examination.

With respect to the private limited purpose bank approach, the Association *notes that*:

- Such approach should be examined more closely to determine whether obstacles to its implementation could be addressed given the potential benefits such approach provides.
- The LP Bank should replicate the current business model of the Clearing Banks by “bundling” clearance and settlement with triparty repo services.
- The possibility of having the Clearing Banks create and initially own the LP Bank should also be considered.⁹

1.5 Old Euroclear Model

As noted in Appendix C, we agree with the White Paper’s conclusion that it is unclear whether this model could adequately address the current system’s shortcomings. Some of the benefits of this approach, as well as potential obstacles to its implementation, are similar in certain respects to that of the private limited purpose bank approach. However, the successful implementation of this approach depends quite heavily upon the willingness of two or more clearing banks to participate and enter into long-term service contracts with a central utility. It is also unclear whether many of the benefits to be gained from this approach could not be accomplished by simply enhancing the current system. Finally, given the potentially limited extent to which such approach could address existing operational vulnerabilities, it is doubtful that the expenditure of potentially significant costs in the implementation of this approach would be justified.

With respect to the old Euroclear model approach, the Association *notes that*:

- Such approach would have to utilize more than one triparty repo service provider in order for it to ensure sufficient intraday financing for the government securities markets.
- Such approach is not as viable an option as improving the existing structure or moving to the private limited purpose bank approach given the apparent obstacles to its implementation and limited benefits such approach provides.

⁹ While we assume for purposes of our analysis of the private limited purpose bank approach that the LP Bank would be owned and governed by a representative group of industry participants as a public industry-owned utility, another approach (the “Modified LP Bank Approach”) that may be worth pursuing would involve having the Clearing Banks (perhaps together with certain custodial banks) form and initially own the LP Bank as a private joint venture or private consortium. Section 6 of Appendix B contains a more detailed discussion of the Modified LP Bank Approach.

1.6 Enhancement of Federal Reserve Services

Enhancing the Federal Reserve System's services to provide additional clearance and settlement functionality would probably provide the greatest reduction of the operational risks inherent in the current system. However, as we discuss further in Appendix D, it may be inappropriate from a public policy standpoint for the Federal Reserve System to extend substantial intraday financing to both dealers and institutional investors. In addition, while some costs may be reduced, others (such as DOD fees) may significantly increase under this approach. There are also concerns relating to the Federal Reserve's responsiveness to customer demand for greater efficiency, reduced fees and new and innovative products and services. Finally, this approach would seemingly require some sort of direct regulation or oversight of the dealers (and perhaps even institutional investors) by the Federal Reserve due to the additional risks posed by allowing such firms direct access to the payment system, thereby creating a new and potentially duplicative regulatory regime.

With respect to the enhancement of the Federal Reserve, the Association *notes that*:

- Further investigation would be needed to address concerns regarding the propriety of the Federal Reserve acting simultaneously as a direct intraday lender to the dealers, a transactional counterparty in open market operations and as a direct or indirect supervisor of the dealers.
- Such approach is not as viable an option as improving the existing clearance and settlement architecture or moving to the private limited bank approach given the obstacles to its implementation and the public policy concerns this approach creates.

* * * * *

The Association believes that the importance of the issues raised by the White Paper become even more evident when viewed in the context of the important roles the government securities markets play. A brief description of the importance of the government securities market is set out below.

2. BACKGROUND

Any proper examination of the benefits to be derived from modifying the existing settlement system architecture must start with recognition of the extraordinary size, liquidity and global importance of this unique market. There is no fixed-income market that is more crucial to the global economy, nor more liquid, than today's primary and secondary market for U.S. government securities.¹⁰ U.S. Treasury securities ("Treasuries") in particular exhibit a high level of liquidity given their low transaction costs and the perception by market participants that such instruments bear no credit risk.¹¹ The liquidity of the Treasury market allows dealers to sell Treasuries without necessarily owning such securities because of the ability,

¹⁰ For example, in the first quarter of 2002, daily trading volume as reported by the primary dealers in Treasury securities averaged \$ 344.8 billion. See Federal Reserve Bank of New York, <http://www.ny.frb.org/pihome/statistics/>.

¹¹ Robert P. O'Quinn, *Economic Benefits From U.S. Treasury Securities*, Report of the Joint Economic Committee, U.S. Congress, 107th Congress, 2nd Session, Feb. 2002 at 2.

under "normal" market conditions, to easily "cover" a short position through the cash, repo or securities lending markets.

In addition to the integral role Treasuries play in the U.S. and global economy, its importance to individual investors and the federal government should also not be underestimated. Yields on government securities are used to set rates on financial instruments of significant importance to individuals, such as mortgages, car loans, and student loans. As the issuer of the world's most liquid debt instrument, the Treasury – and thus indirectly U.S. taxpayers - benefits from the presence of this liquid secondary market by receiving the lowest financing costs available. Economists today generally acknowledge that market participants will pay a liquidity premium¹² in order to obtain a particularly liquid financial asset.¹³ The Treasury captures this premium whenever it auctions new securities. It is not surprising, therefore, that Treasuries are the most widely held debt securities in the world.¹⁴

The active repurchase ("repo") and securities lending market in government securities also plays an important role in our financial markets and our economy. For instance, the FRBNY utilizes government securities in the conduct of its open market operations, which are used to adjust the Federal Funds rate to meet the Fed Funds target set by the Federal Reserve System's Federal Open Market Committee. The success of these open market operations depends on the ability of the primary dealers to "reverse in" or "repo out" billions of dollars worth of government securities each business day.¹⁵

As important as the government securities trading markets are to Wall Street and Main Street alike, market participants also rely significantly on the proper functioning of the clearance and settlement system supporting these markets. While the tragic events of September 11, 2001 demonstrated that the cash and repo markets for government securities can still function (albeit with diminished liquidity) when the clearance and settlement system remained subject to a back-log of unsettled trades,¹⁶ a substantial and sustained impairment of such system

¹² Robert P. O'Quinn, *Economic Benefits From U.S. Treasury Securities*, Report of the Joint Economic Committee, U.S. Congress, 107th Congress, 2nd Session, Feb. 2002 at 2-4. See Yakov Amihud and Haim Mendelson, "Liquidity, Maturity, and the Yields on U.S. Treasuries," *Journal of Finance* 46 (September 1991): 1411- 1425; Avraham Kamara, "Liquidity, Taxes, and Short-Term Treasury Yields," *Journal of Financial and Quantitative Analysis* 29 (September 1994): 403-417; Francis A. Longstaff, "The Flight-To-Liquidity Premium in U.S. Treasury Bond Prices," *University of California Los Angeles Working Paper* (May 2001).

¹³ Of course, investors are also attracted to Treasuries for other reasons. As noted above, they are regarded as free from any credit risk. In light of this fact, many institutional customers are attracted to Treasuries because they are an excellent vehicle for hedging interest rate exposures. A large supply of actively traded Treasuries allows financial market participants to develop a "true" credit risk-free yield curve, thereby facilitating more efficient pricing of financial instruments and allowing financial institutions to hedge interest rate risk more effectively. Such instruments also provide a liquid source of collateral for such institutions to pledge in swaps and other derivatives transactions and as a vehicle to obtain funding or other securities to fulfill their numerous financial obligations. *Id.*

¹⁴ Robert P. O'Quinn, *Economic Benefits From U.S. Treasury Securities*, Report of the Joint Economic Committee, U.S. Congress, 107th Congress, 2nd Session, Feb. 2002.

¹⁵ It is important to recognize that the cash and repo markets in Treasuries play similarly important roles in the functioning of economies around the globe; in a recent report, it was estimated that foreign institutions held 37% of all outstanding U.S. Treasury securities. See FRBNY Report (June 6, 2002), available at <http://www.federalreserve.gov/releases/Z1/Current/z1r-4.pdf>.

Interagency White Paper Response
 August 19, 2002
 Page 9

can ultimately lead to a significant adverse impact on trading in the government securities markets. Moreover, perceptions of instability in the clearance and settlement system can itself lead to impaired liquidity.¹⁷

It is therefore imperative that every effort be made to ensure that the government securities clearance and settlement system functions properly *both in times of relative normalcy, and in times of stress*, in order to guarantee that the government securities market continues to fulfill its several important functions. In this regard, the Association recognizes that the continued development of robust back-up facilities, joint data repositories and coordinated contingency planning by the Clearing Banks, DTCC, the dealers and other key participants in the government securities market is essential.¹⁸ However, the events of September 11, 2001, also highlighted the fact that the current clearance and settlement system - including the operational aspects, trading practices and regulatory framework - were sufficiently flexible to allow market participants, regulators and key providers of clearance and settlement services to work efficiently together to quickly minimize the disruptive impact of the September 11 terrorist attacks.¹⁹

* * * * *

The Association believes that the examination of the current clearance and settlement structure, as well as any alternative structures, should be undertaken against a framework of commonly accepted benchmark goals and objectives. We respectfully suggest that you consider utilizing the following analytical framework.

¹⁶ See, generally, "Treasury Market is Faced with Incomplete Trades," The New York Times, October 3, 2001; Minutes of Emergency Meetings of The Bond Market Association, September 11-21, 2001, available at: http://www.bondmarkets.com/market/9-11_minutes.shtml.

¹⁷ It is the Association's understanding that there was substantial evidence that certain participants in the securities lending markets withdrew from lending their government securities in the days following the attacks thereby reducing liquidity. See "Summary of Lessons Learned and Implications for Business Continuity," Discussion Notes at 2 (Feb. 13, 2002), ("Other institutions and their customers built up high cash balances or held on to government securities positions for precautionary reasons, exacerbating market liquidity imbalances"), available at: <http://www.ny.frb.org/bankinfo/payments/discussion.pdf>. [hereinafter "Business Continuity Summit Staff Notes"].

¹⁸ The Association also believes that implementation of certain netting arrangements among dealers and customers might also further enhance liquidity particularly in times of market stress. In 2000, the Association formed a Task Force specifically to look into this issue. Presently, our STP/T+1 Steering Committee, our MBS/ABS Securities Division and the Asset Managers Forum are all continuing to explore this idea.

¹⁹ For instance, despite the lingering difficulties in the operating and reconciliation environment in the weeks following September 11, 2001, GSCC continued to successfully compare submitted trades, net down the obligations of each of its members and novate the relevant transactions. GSCC's ability to perform such functions was facilitated by certain interim trading and settlement recommendations issued by the Association. These recommendations included: (i) a recommended T + 5 settlement cycle for all secondary market cash transactions in Treasury and agency securities (excluding discount notes); (ii) a limitation on substitutions of securities in repo transactions, and (iii) a moratorium for certain blind-brokered repo transactions submitted to GSCC. See Minutes of Emergency Meetings of The Bond Market Association, *supra* note 15; see also Government Securities Clearing Corporation, Important Notice GSCC073.01 dated Sept. 19, 2001, available at: www.gsc.com.

3. METHODOLOGY FOR THE EXAMINATION OF A GOVERNMENT SECURITIES CLEARANCE AND SETTLEMENT SYSTEM

We believe that the following criteria, *in order of priority*, represent the guiding principles that the Agencies and market participants should look to in assessing what form of clearance and settlement system can best support the primary and secondary market in government securities:

- Sufficient funds and securities must be available to market-makers, not only in "normal" market conditions, but also in times of market stress, to support a deep, liquid and transparent trading and funding market.
- Operational and exit risks that could disrupt the clearance and settlement process must be adequately mitigated.
- Incentives should exist for service providers to pursue innovations and invest in research and development (resulting from technology advances or trading practice advances) that are necessary to respond to the needs of market participants.
- The costs of operating the clearance and settlement system (including conversion costs associated with alternative or structural changes) should be reasonable and efficiently borne relative to the benefits afforded market participants.

3.1 Sufficient funds and securities must be available to market-makers, not only in "normal" market conditions, but also in times of market stress, to support a deep, liquid and transparent trading market.

The government securities markets currently enjoy a high level of liquidity²⁰ which, in turn, provides dealers with the ability to promptly fulfill their numerous financial obligations, including the ability to: (i) borrow securities to cover short positions; (ii) obtain needed cash to finance the outright purchase of securities; and (iii) obtain government securities to pledge as collateral in order to borrow other types of securities needed for delivery or to post as collateral for other types of obligations, such as to counterparties in derivatives transactions and to exchanges and clearinghouses.

Given the enormous volume of daily trading activity in government securities²¹ and the importance of continued liquidity to the various roles the government securities market plays, it is imperative that financial institutions – and in particular market makers such as dealers –

²⁰ For the purposes of this letter, we use the term "liquidity" to describe how easily a government security can be converted to cash. As discussed throughout our response, the Association believes the provision of adequate intraday financing by a government securities clearance and settlement structure is a key factor in maintaining the high level of liquidity in the government securities markets.

²¹ According to statistics issued by GSCC, \$153.4 trillion of Treasuries were utilized in repurchase ("repo") transactions in 2001 indicating an average daily trading volume of approximately \$600 billion. In addition, GSCC recently experienced a record level of volume, netting over \$5 trillion worth of trading activity. See GSCC Important Notice, "A Five Trillion Dollar Day," August 16, 2002, available at http://www.gsccl.com/important_notices_frame.html.

Interagency White Paper Response
 August 19, 2002
 Page 11

operate in a trading environment where they feel confident that their contractual obligations to buy or sell securities will be satisfied on the settlement date for such trades, and that fails²² which occur in the normal course of dealings can be promptly reconciled and ultimately settled.²³

The smooth functioning of the settlement system and the ample availability of funds and securities is also important to the reduction of systemic risk due to the interconnected nature of the financial obligations that exist among participants in the government securities market. Often, dealers are dependent upon receiving funds or securities from another financial institution in order to meet their own obligations. The failure by one dealer to receive expected funds or securities from a financial institution may cause it to fail on its obligations to another dealer, potentially leading to a chain of fails.²⁴

The provision of intraday financing by a government securities clearance and settlement system is also an integral part of maintaining liquidity in the secondary market for government securities, both in times of relative normalcy and in times of severe market stress. "Intraday financing" essentially involves providing a financial institution with the means to obtain and utilize securities without immediately paying for such securities, and allowing such dealer to pay for - or return - such securities before the end of the day. In light of the enormous volume of trading in the government securities markets and the interconnected nature of obligations in such markets, it is imperative that dealers have access to adequate intraday financing in order to allow them to promptly obtain and deliver government securities throughout the business day.²⁵

²² It is important to note that fails often occur in the ordinary course of trading in the government securities markets (including both the cash and repo markets). However, a disproportionately high level of fails can cause a severe reduction in liquidity, raising the potential for systemic risk. For example, based on reports we have received from GSCC and market participants, the government securities markets may experience \$1-3 billion in fails each day under "normal" market conditions. However, the market experienced a high of \$190 billion in fails on an average basis in the weeks immediately following September 11, 2001. This contributed to an overall reduction in liquidity in the marketplace which, in turn, led to a same-day auction by the Treasury of \$6 billion of 10-year notes in an effort to alleviate this situation. See e.g. "Treasury Market is Faced with Incomplete Trades," The New York Times, October 3, 2001.

²³ In addition to the need to fulfill delivery obligations promptly, broker-dealers may also be adversely affected by outstanding fails pursuant to certain regulations. See e.g., 1934 Exchange Act Rule 15c3-1 (requiring a broker-dealer to deduct from its net capital outstanding fails which exceed a certain length of time); 1934 Exchange Act Rule 15c3-3 (requiring cash and/or qualified securities to be maintained in a "Special Reserve Bank Account for the Exclusive Benefit of Customers" in connection with certain outstanding fails and unresolved reconciliation differences with accounts, clearing corporations, or depositories).

²⁴ Congress and other policymakers have long recognized that certain interrelated financial activities and markets have the potential to create broader systemic risk. Systemic risk arises when a disruption at a firm, in a market segment, or to a settlement system causes widespread difficulties to other markets or the financial system as a whole. In order to minimize the risk of such systemic events, the Bankruptcy Code, the Federal Deposit Insurance Act ("FDIA") and the Federal Deposit Insurance Corporation Improvement Act ("FDICIA") each contain provisions protecting the right of financial institutions and certain other creditors to terminate, close out and net financial contracts with an insolvent entity in a timely manner. See e.g. Bankruptcy Code Sections 555, 556, 559, 560, 362(b)(6),(7) and (17), 546(e),(f) and (g). See also FDIA Section 11(e)(8); 12 U.S.C. 4401 et seq.

²⁵ The importance of intraday financing to the government securities markets is widely acknowledged and was highlighted in the "Vision 2000" project which also sought to facilitate changes to the existing government securities clearance and settlement system. This project, initiated by the National Securities Clearing Corporation (NSCC) in 1996, contemplated the creation of a structure similar to the "old Euroclear model"

The provision of intraday financing takes a number of forms. The most straightforward manner of intraday financing is the extension of unsecured and secured intraday credit by a financial institution lender (which may or may not be the clearance and settlement facility) to a dealer or other market participant. In the current structure, this intraday credit is readily available, in part, because the Clearing Banks can, if necessary, temporarily draw down their accounts at the FRBNY and incur daylight overdraft ("DOD").²⁶ Some of this intraday credit, in turn, is utilized by dealers through their accounts at the Clearing Banks when purchasing government securities when they do not have sufficient funds to do so.²⁷ It is our understanding that the two Clearing Banks each extend approximately \$1 trillion in intraday credit to their dealer/clearing customers each day.²⁸

The Clearing Banks also provide intraday financing by allowing a dealer the use of securities on an intraday basis in connection with triparty repo services offered by the Clearing Banks. The securities sold (or "repoed") by a repo seller and cash used to purchase (or "reverse in") the repoed securities by a repo buyer are placed in a triparty custody account, usually with the dealer's Clearing Bank, which provides essential administrative functions, including the allocation of repoed securities in accordance with guidelines set by the repo buyer, and revaluing (or "marking-to-market") of securities in the triparty repo facility. On the day of a repo trade, by day's end, the triparty custodian transfers the repoed securities from the dealer's proprietary account to a custody account maintained by the triparty custodian on behalf of the repo buyer. The following morning, the triparty repo "unwinds", and in simultaneous transfers the repo securities are returned to the repo seller/dealer and the cash used to purchase such securities is returned to the repo buyer. The repo seller/dealer thereby has access to its securities during the day and can use them intraday to make

discussed in the White Paper. While the proponents of this project believed that it would reduce certain costs associated with the clearance and settlement process, others believed at that time that such structure would adversely impact the provision of intraday financing to clearance participants. Given such concerns, the Vision 2000 project was shelved in 1997.

²⁶ The most recent version of the Board's Payments System Risk (PSR) policy (effective December 10, 2001) (the "PSR Policy") limits the maximum amount of DOD a depository institution may incur by imposing a limit – or "net debit cap" – on each depository institution, including the Clearing Banks; however, depository institutions may exceed their net debit caps, to an extent, by pledging collateral for overdrafts in excess of their caps.

²⁷ The Fedwire payments system is "passive to the receiver" of securities; in other words, the purchaser of securities is automatically debited funds from its account at the Clearing Banks upon the receipt of securities. As such, in a situation where such purchaser has insufficient funds at the moment it receives securities, the provision of intraday credit is essential to ensure that the bonds are not "DK'd" and the purchaser is able to pay for such securities even if the purchaser has insufficient funds in its account.

²⁸ To the extent a clearance and settlement facility provides intraday financing to a dealer, such a facility is exposed to the risk that such dealer will fail. In such an event, the clearance facility's exposure would be measured by the extent of intraday financing extended by the clearance facility to the dealer, minus the liquidation value of any collateral that the clearance facility may have held for the provision of such intraday financing. In addition to requiring collateral for the extension of intraday credit, this risk can be mitigated through an evaluation of the creditworthiness of the dealer being financed. More stringent controls could take the form of a limitation on the provision of unsecured intraday credit; increased collateralization requirements to obtain intraday credit; limitations on or elimination of unsecured extensions of intraday credit; elimination of any "subjective" discretion to extend such intraday credit; and limitations on the amount of other forms of intraday financing (such as limits on the amount of securities a dealer may use intraday during the "unwind" of a triparty repo). However, the imposition of rigid credit risk mitigation controls may have the effect of reducing the amount of intraday financing by the clearance facility to such an extent as to cause a potentially problematic reduction of secondary market liquidity.

deliveries in connection with its trading and financing activities. The triparty custodian through its management of the transfer process essentially finances the dealer's securities intraday. Under circumstances in which the repo buyer leaves the cash it used to purchase securities in its triparty account intraday (as could be the case in connection with a term repo transaction), no DOD is incurred by the triparty repo provider, or passed along to the repo seller. However, in cases where the repo buyer removes such cash from the triparty repo facility (as could be the case in connection with an overnight repo transaction or a transaction that is otherwise closing-out), the repo seller's overdrafts are not funded by such cash in the repo buyer's triparty account, and such triparty custodian/repo provider may incur a DOD from the FRBNY; if so, it would pass along such credit - and the attendant DOD fees it incurs - to the repo seller.

For all the above reasons, the Association believes that any restructuring of the clearance and settlement system must, at a minimum, guarantee that such system continues to provide sufficient intraday financing to dealers.

3.2 Operational and exit risks that could disrupt the clearance and settlement process must be adequately mitigated.

While the Association believes that the reduction of operational risk²⁹ or exit risk³⁰ in any clearance system is an important factor in reviewing how such system should be ideally structured, we believe that it should not be the sole - or even the determinative - factor. As discussed in detail above, we believe that the adequate provision of intraday financing by a clearance system should be the primary factor taken into account in examining a government securities clearance system.

Exit risk and operational risk can be present in a number of forms. In addition to the risk of a voluntary exit by a clearance facility, the involuntary exit of such facility may occur as a result of financial difficulties experienced by such facility, either in connection with or apart from the clearance and settlement of government securities (e.g. the insolvency or the criminal indictment, guilty plea or conviction of a provider of clearance services). Operational risk can arise from a physical disruption at a primary or backup facility (e.g. a power or communications outage or physical damage experienced at a clearance facility).³¹

Operational and exit risks can be mitigated in a number of different ways. For example, operational risk can be mitigated through the creation of redundant lines of communication that are not in close physical proximity to one another and utilization of multiple primary sites or active ("hot") back-up facilities that could operate should the main funds or securities

²⁹ For the purposes of this letter, we use the term "operational risk" to refer to a temporary and material disruption in the physical or technological operations of a clearance facility or other key service provider.

³⁰ For the purposes of this letter, we use the term "exit risk" to refer to the potential for the permanent cessation of functioning of a particular clearance and settlement facility, whether brought about by a voluntary exit from the business, the existence of significant financial or legal difficulties or the insolvency of such facility.

³¹ The events surrounding September 11, 2001 and the temporary disruption of services are an example of the operational risk present in the current government securities clearance and settlement system. Of course, such an event can also indirectly create exit risk to the extent a provider elects not to resume business after suffering a severe operational disruption.

clearance facility become inoperable. The potential for a clearance facility to experience financial difficulties resulting from financial transactions apart from the clearance of government securities may also be mitigated or eliminated by limiting the activities of a clearance facility to the clearance and settlement of government securities and related services.

It is clearly important that any potential for systemic disruptions to the financial markets and payments systems should be minimized where possible. However, while it is imperative that operational and exit risks are adequately managed, the Association believes that a successful clearance and settlement system must seek to prudently manage these risks without adversely impacting the operation of the clearance and settlement system by, for example, unduly restricting intraday financing.

3.3 Incentives should exist for service providers to pursue innovations and invest in research and development (resulting from technology advances or trading practice advances) that are necessary to respond to the needs of market participants.

The Association believes that incentives to innovate clearance and settlement functionalities and risk mitigation controls must be present in any potential clearance and settlement system in order to adequately address the inherent risks in such system, to continue to provide necessary liquidity, and to maintain a reasonable level of fees with regard to the operation of such system. While such incentives to innovate may come from competitive pressures between clearance facilities, a governance structure that involves the participation by the dealer community may also provide the necessary incentives for innovation. In short, the context in which a clearance system operates must encourage service providers to continuously improve their systems.³²

Fortunately, both GSCC and the Clearing Banks have demonstrated a strong tendency to provide new and innovative services. For instance, in late 2000, GSCC rolled out a new real time trade matching system³³ that facilitates prompt matching and confirmation of transactions on a real-time basis.³⁴ Likewise, the Clearing Banks not only helped develop the

³² The Association is not commenting at this time on whether the current structure of the marketplace for providing government securities clearance services is, in fact, the most efficient structure possible. We do believe that market forces have "naturally" helped evolve the clearance and settlement of government securities in the U.S. to a state where there are only two major clearance facilities. As with most industries, the nature of technology and associated costs, together with demand, are also important determinants of market structure. Specifically, if the technology is such that a typical firm's average costs decline over a broad range of output levels, it may be efficient for a limited number of firms to supply total industry output. In the extreme, a "natural monopoly" may minimize the costs of producing total output demanded. . In the case of clearing and settlement facilities, therefore, substantial economies of scale and scope may have caused the current concentrated industry structure to emerge. See, e.g., Robert S. Pindyck and Daniel L. Rubinfeld, *Microeconomics* (New York: Macmillan Publishing Company, 1989), at 354-355, (discussing natural monopolies and the regulation thereof.); Alexis Jacquemin, *The New Industrial Organization: Market Forces and Strategic Behavior*, translated by Fatemeh Mehta (Cambridge, MA: MIT Press, 1987), at 23.

³³ See Government Securities Clearing Corporation Important Notice: "Interactive Messaging For Real-Time Trade Comparison to be Implemented November 17, 2000; Doc. GSCC085.00, October 26, 2000.

³⁴ This service helped prevent broader reconciliation problems at GSCC stemming from incomplete trade information in the days following the September 11, 2001 attacks, given that it helped ensure that transactions entered into prior to the intraday disruption in the clearance system still had a confirmed counterparty match for all trades submitted to GSCC up to the point of such disruption.

concept of utilizing a triparty custodian to engage more efficiently in repo transactions, they also worked closely with GSCC to support the introduction of GSCC's general collateral finance ("GCF") Repo service.³⁵

3.4 The costs of operating the clearance and settlement system (including conversion costs associated with alternative or structural changes) should be reasonable and efficiently borne relative to the benefits afforded market participants.

As set out below, there are a number of costs associated with the clearance and settlement of government securities. Certain of these costs are "discretionary", in the sense that they are commercially determined by a clearance facility. Other costs are dictated by the Board and the FRBNY, and in this manner are "non-discretionary" costs.³⁶ Discretionary fees include clearing fees charged by a clearance facility on a per-transaction basis. Triparty repo fees are typically based on a combination of a per-transaction fee and a fee based on a percentage of the dollar volume of triparty repo transactions conducted. Fixed fees include DOD fees, which are determined by the Board's Payment Systems Risk (PSR) Policy.³⁷ Transactions which utilize the Fedwire are also assessed a fee on a per-transaction basis that is fixed by the FRBNY.³⁸

³⁵ See Government Securities Clearing Corporation Important Notice: "GCF Repo Service Implementation"; Doc. GSCC093.98, November 13, 1998.

³⁶ In addition, there are benefits that if not retained would be a "cost." For example, a dealer receives balance sheet relief under Financial Accounting Standards Board Interpretation No. 41 ("FIN 41") depending in part on the manner in which securities are cleared. Under FIN 41, a financial institution may offset amounts recognized as payables and receivables that represent repos and reverse repos with the same counterparty for accounting purposes if they meet certain requirements specifically: (i) the repo and reverse repo are executed with the same counterparty; (ii) the repo and reverse repo have the same settlement date; (iii) the repo and reverse repo are executed under a master netting arrangement; (iv) the underlying securities exist in "book entry" form and can be transferred only by means of entry in the record of the transfer system operator or securities custodian; (v) the repo and reverse repo are settled on a securities transfer system, and the bank has associated banking arrangements in place; and (vi) the bank intends to use the same account at the clearing bank or other financial institution at the settlement date in transacting both (a) the cash inflows resulting from the settlement of the reverse repo and (b) the cash outflows in settlement of the offsetting repo. While the Association wishes to call the attention of the Agencies to the benefits of FIN 41, we are not commenting at this time on whether any of the proposed clearance system alternatives discussed in the White Paper would meet the requirements set out under FIN 41.

³⁷ Federal Reserve DOD fees are calculated on a daily basis and are equal to the effective daily rate charged for daylight overdrafts multiplied by the average daylight overdraft for the day minus a deductible valued at the effective daily rate. The Board has considered implementing a two-tiered DOD fee structure, which potentially would involve assessing lower fees for the use of collateralized DOD by depository institutions. See "Potential Longer-Term Policy Direction," Docket No. R-1111, available at: <http://www.federalreserve.gov/boarddocs/press/boardacts/2001/20010530/>. The Association has expressed its support for such proposal. See Comment Letter from the Association, dated December 21, 2001, on the Board's Potential Longer-Term Policy Direction, available at: <http://www.bondmarkets.com/regulatory/fund.shtml>.

³⁸ Under Operating Circular 7, the Reserve Banks may set certain fees for the transfer of Fedwire Book-Entry Securities. The fees set by the FRBNY are available at: <http://www.frbservices.org/Book-Entry/FeeSchedBook.cfm>.

The Association believes that the reduction of costs in the clearance and settlement of government securities would benefit the financial markets by allowing dealers to utilize capital that would otherwise be devoted to clearance-related fees.³⁹ While costs should not be a determinative factor in reviewing how a clearance and settlement system should be structured, it is clear that they should always bear some reasonable relationship to the benefits being conveyed to market participants.

Finally, additional costs may arise, in the context of an industry-owned utility, from clearing fund⁴⁰ and other margin requirements imposed on clearing members, as well as from "loss sharing" arrangements utilized by such facilities that could indirectly burden participants. Typically, a commonly owned utility will employ such loss mitigation practices to protect it and its members from the failure of one or more of its members. To the extent the collateral contained in the failed member's margin fund and clearing fund accounts are insufficient to fully cover the failed member's reimbursement obligation to the utility, there are additional layers of protection before a reimbursement obligation is imposed on the clearing members generally. However, assuming that these facilities utilized adequate risk management systems and marked-to-market the collateral they collected from clearing members, it would be unlikely that such loss sharing arrangements would add substantially to the costs of utilizing the utility.⁴¹

* * * * *

By applying the above principles to the current clearance system and the alternatives set out in the White Paper, our conclusion at this time is that the risks in the current system should be addressed while retaining the structure of the current system, at least in the short term. Although the Association believes that the long-term strategy for the industry should include exploring alternative clearance and settlement arrangements, including those outlined in the White Paper, our initial review suggests concerns with the ability of alternative structures to provide sufficient intraday financing to the government securities markets.

³⁹ In this regard, it is interesting to note that one of the main impetuses for restructuring the pan-European trading and settlement systems is to reduce the post-trading costs of clearing, settling and safekeeping securities. See Linda Goldberg, John Kambhu et.al. "Securities Trading and Settlement in Europe: Issues and Outlook" in current Issues in Economics and Finance: April 2002; Volume 8 Number 3 at 2 [hereinafter "Goldberg & Kambhu"].

⁴⁰ For instance, GSCC requires its clearing members to maintain certain clearing fund margin in order to have on deposit from each netting member funds sufficient to satisfy any losses that may otherwise be incurred by GSCC (and its members) as a result of such member's default as well as to ensure that GSCC has sufficient liquidity to meet its payment and delivery obligations.

⁴¹ Thus, for instance, only those members at GSCC that dealt with a defaulting member prior to its default will be asked to help satisfy in full the loss to GSCC on a pro rata basis (based on the amount of trading activity each member had with the defaulting member) if the margin posted by the defaulting member was insufficient to cover GSCC's loss upon liquidation of the defaulting member's positions. Likewise at GSCC, only if one of those members that traded with the defaulting member prior to its default itself fails to pay in full its allocation, would other members be asked to generally share in the remaining loss. See, e.g. "GSCC Rulebook," Rule 4, *Clearing Fund, Surveillance Status and Loss Allocation*, p. 63, available at http://www.gsc.com/important_notices_frame.html.

A detailed evaluation of the current system and the alternatives described in the White Paper is set out in the attached appendices. However, given our view that the current system should not be artificially restructured, at least in the short term, we would like to close by noting specific conclusions we have reached with respect to enhancing the current clearance and settlement system.

4. ENHANCING THE CURRENT SYSTEM

4.1 The Current Government Clearance and Settlement System Allows For a High Level of Liquidity in the Government Securities Markets by Providing an Adequate Amount of Intraday Financing to Dealers.

As mentioned earlier, the Association is convinced that the critical importance of dealer access to sufficient intraday financing dictates that the risks inherent in the current system can and should be addressed without fundamentally modifying the current settlement architecture. There is a clear and unambiguous relationship between the uniquely liquid secondary market for government securities in this country and the availability of adequate levels of intraday financing currently provided by the Clearing Banks. The current system facilitates a high level of liquidity in the government securities markets through the provision of an adequate amount of intraday financing, including secured and unsecured extensions of intraday credit through DOD, triparty repo, and intraday securities lending. The difficulty that alternative structures may have in providing similar amounts of intraday financing strongly suggest having the industry focus initially on addressing the risks inherent in the current system and not on fundamentally altering the existing clearance and settlement system.

The Clearing Banks currently provide crucial intraday credit to the dealers on both an unsecured and secured basis, and this credit extension involves a comprehensive review by the Clearing Banks of such dealer's creditworthiness and the dealer's ability to provide collateral to the Clearing Banks. In addition to providing standing lines of secured and unsecured intraday credit, it is our understanding that the Clearing Banks also provide additional settlement-related credit depending on a dealer's past history with the Clearing Bank, and current potential exposure as a result of its settlement activities. This aspect of the current system is critically important because it allows for needed flexibility in the provision of intraday credit, given that the availability of credit to market-makers is based not just on the Clearing Banks' settlement services but also on the broader financial relationship each Clearing Bank has with its dealer/customers.

4.2 The Current Government Securities Clearance and Settlement System Presents a Level of Operational and Exit Risk that Can be Managed within the Existing System

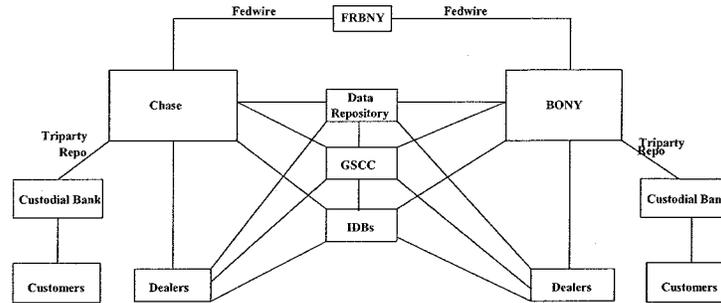
The events of September 11, 2001 not only served as a painful reminder that our financial markets depend upon the smooth functioning of the securities clearance and settlement infrastructure, but also that such infrastructure was reliant on the interdependent operations of critical service providers. This highlighted the fact that the specific disaster recovery capabilities and level of preparedness at a few key institutions could significantly impact not only the dealers and investors that rely on such institutions for clearing and triparty repo services but also the government securities clearance and settlement system as a whole.

Fortunately, as explained in Appendix A, many of the specific vulnerabilities that were highlighted in our system by the events of September 11 are capable of being addressed without having to fundamentally alter the system's current architecture. The Clearing Banks (as well as other industry participants, such as DTCC and the dealers), continue to improve their contingency and back-up arrangements through, for example, the creation of multiple "hot" back-up sites. Notwithstanding these efforts, the Association believes additional steps can be taken to mitigate operational risk, particularly in connection with the development of common communication protocols to facilitate the transfer, if necessary, of information from one Clearing Bank to another, as well as "redundant connectivity" between the dealer community and the Clearing Banks. The Association believes voluntary and involuntary exit risk can be mitigated by private bilateral assurances from the Clearing Banks to their customers and the broader regulatory community that they will continue to provide clearance and settlement services. Notwithstanding these assurances, the development of an unwind plan should be explored to ensure the orderly closure and transfer of clearance services in the event of an exit by one of the Clearing Banks. With regard to all of the above solutions, the Advisory Committee would play a crucial role in examining and further developing the Association's proposed solutions.

We also believe it is important that institutions that play a critical role in the current clearance and settlement system should be recognized as such from a regulatory standpoint and be held to a higher standard in terms of their recovery capabilities. For instance, given the unique role the Clearing Banks currently play in the government securities clearing system, it might be appropriate to revise certain banking regulations that currently apply to the Clearing Banks to more formally acknowledge their special status. A regime for designating and regulating a bank as a "primary clearing bank" might even be structured in a manner that is similar to being identified currently by FRBNY as a primary dealer. Likewise, the Board's current PSR Policy could be modified to specifically recognize the special status that the Clearing Banks currently occupy in the clearance and settlement of government securities. Such special regulatory status could enhance the franchise value of the Clearing Banks' functions and may, in turn, provide sufficient economic incentive for other banks to compete with the Clearing Banks in providing clearance services. In addition, such clarifications could also provide incentives for another bank to acquire a Clearing Bank in the event of a voluntary or involuntary exit by one of the Clearing Banks.

4.3 Creation of a Data and Software Repository May Also Alleviate Problems Arising from the Exit of a Clearing Bank, While Maintaining the Level of Intraday Liquidity under the Current System.

We believe that an important step towards a more coordinated and comprehensive industry-wide contingency plan may be the creation of a shared backup data repository (the "Data Repository"). As outlined below, this Data Repository would serve as a repository for maintaining, on a real-time basis, "mirror image" data files containing the positions of dealers both inter-Clearing Bank and intra-Clearing Bank.



With the existence of the Data Repository, a rapid switching of positions from one Clearing Bank could be facilitated. The Data Repository could thus ensure prompt recovery by both Clearing Banks as the settlement processing for one Clearing Bank could be stored in the Data Repository. This would allow many of the benefits of the current system – particularly the provision of intraday financing – to remain the same, while still mitigating certain operational risks present in the current system.

The most significant obstacle to the implementation of a Data Repository is the cost that would be incurred in order to implement such an approach. Even assuming that such Data Repository would be formed as an expansion of an existing utility, the costs involved in creating a facility that would reflect, in real-time, positions both inter- and intra-Clearing Bank could potentially be very high. In addition, it is likely that in order for the Data Repository to accurately reflect the positions of dealers within a Clearing Bank, dealers would need to connect to such Data Repository, in addition to their Clearing Bank, in order for the Data Repository to track positions internal to the Clearing Banks. Such additional connectivity from the dealers to the Data Repository would potentially amount to a significant expenditure on the part of the dealers to rework their operational infrastructure to establish the necessary connectivity to the Data Repository.

In sum, creating a common Data Repository could help reduce some of the more significant risks inherent in the current system while retaining the benefits of the current system. However, while the Association believes that this approach holds the potential for resolving a number of significant issues present in the current clearance and settlement structure, it is unclear whether the potentially high conversion costs of implementing such approach would justify the benefits that it would present.

5. CONCLUSION

The Association greatly appreciates the opportunity to comment on an issue of such significance not only to the government securities markets, but also to the U.S. and global economy, and to large financial institutions and individual investors alike. The numerous issues raised by the White Paper cannot, of course, be thoroughly addressed within the space of our letter or within the attached appendices, which present a more detailed analysis of the current system and the alternatives set out in the White Paper based on the

Interagency White Paper Response
 August 19, 2002
 Page 20

methodology set out above. The Association hopes that our response will serve as a useful framework in addressing these issues, and further assist the Agencies and any future Advisory Committee in their continuing examination of the government securities clearance and settlement system. In this regard, the Association stands ready to assist in providing whatever additional input the Agencies may wish to obtain with regards to their examination.

As we approach the one year anniversary of the September 11, 2001 terrorist attacks, the Association, with due reflection, would also like to acknowledge the extraordinary assistance and support both of your organizations, the Treasury and the FRBNY provided the Association, its staff and its members in the days and weeks that followed the tragedy. We feel strongly that our shared history of working together with you in an open and cooperative manner helped facilitate the rapid resumption of trading in the government securities market. In that regard, we look forward to once again working with you as the evaluative process continues to ensure an efficient, cost-effective and reliable government securities clearance and settlement system for all market participants.

Please feel free to contact Paul Saltzman (212.440.9459), Omer Oztan (212.440.9474) or Eric L. Foster (212.440.9448) at the Association should you have any questions or comments regarding our response.

Sincerely,

/s/ Thomas C. Connor

/s/ Thomas G. Wipf

Thomas C. Connor, *Managing Director*
 JP Morgan Chase & Co.
 Chairman
 Primary Dealers Executive Committee

Thomas G. Wipf, *Managing Director*
 Morgan Stanley & Co. Inc.
 Chairman
 Funding Division Executive Committee

/s/ Thomas J. Paul

/s/ Robin Vince

Thomas J. Paul, *Managing Director*
 Deutsche Banc Alex. Brown
 Vice Chairman
 Primary Dealers Executive Committee

Robin Vince, *Vice President*
 Goldman, Sachs & Co.
 Vice Chairman
 Funding Division Executive Committee

Interagency White Paper Response
August 19, 2002
Page 21

Is/ Frank DiMarco

Frank DiMarco, *Managing Director*
Merrill Lynch & Co., Inc.
Chairman
Interagency White Paper Response Task Force

cc: *Board of Governors of the Federal Reserve System*
Roger Ferguson, *Vice Chairman*
Patrick Parkinson, *Associate Director*
Jeff Stehm, *Assistant Director*
Patricia White, *Assistant Director*

Securities and Exchange Commission
Annette L. Nazareth, *Director*
Robert Colby, *Deputy Director*
Larry E. Bergmann, *Senior Associate Director*
Jerry W. Carpenter, *Assistant Director*
Jeffrey Mooney, *Senior Special Counsel*

Treasury Department
Brian C. Roseboro, *Assistant Secretary for Financial Markets*
Norman Carleton, *Director of Federal Finance Policy Analysis*

Bureau of Public Debt
Lori Santamorena, *Executive Director*
Carl M. Locken Jr., *Assistant Commissioner*

Federal Reserve Bank of New York
Joyce Hansen, *Deputy General Counsel and Senior Vice President*
Darryll Hendricks, *Senior Vice President*

Federal Deposit Insurance Corporation
Michael H. Krimminger, *Senior Policy Analyst*

European Central Bank
Niall Lenihan, *Senior Legal Counsel*

Group of Thirty
John Walsh, *Executive Director*

The Bank of New York
Art Certosimo, *Senior Vice President*

JP Morgan Chase
Allen B. Clark, *Senior Vice President*

Depository Trust & Clearing Corporation
Dennis J. Dirks, *President & C.O.O.*
Thomas F. Costa, *President & C.O.O.*
Jeffrey F. Ingber, Esq., *Managing Director & General Counsel*

Interagency White Paper Response
 August 19, 2002
 Page 22

Securities Industry Association (SIA)

Donald Kittell, *Executive Vice President*
 Thomas J. Monahan, *Assistant Vice President*
 Mike Viviano, *Chair, SIA Operations Committee,*
Executive Vice President, The Bank of New York

Investment Company Institute

Amy Lancellotta, *Senior Counsel*

Asset Managers Forum

Michael L. Wyne, *Chair, Managing Director, Fischer, Francis, Trees & Watts*
 Kenneth Juster, *Director*

European Securities Forum

Joan Beck, *Chairman*

The Bond Market Association

Board of Directors

Tom Kalaris, *Chair, Chief Executive, Americas, Barclays Capital*
 Herbert McDade, *Vice Chair, Managing Director, Lehman Brothers*

Interagency White Paper Response Task Force

Primary Dealers Executive Committee

Primary Dealers Committee

Federal Agency Committee

Mike Graf, *Chair, Managing Director, Merrill Lynch & Co., Inc.*
 Jeff Carleton, *Vice Chair, Managing Director, Salomon Smith Barney*

Funding Division Executive Committee

Funding Division Legal Advisory Committee

Sibyl Peyer, *Chair, Vice President and Associate General Counsel,*
Goldman Sachs & Co.

Marianna Maffucci, *Director and Senior Counsel, Deutsche Bank Securities*

Government Division Legal & Compliance Committee

Andrew Alter, *Chair, Managing Director and Counsel, Salomon Smith Barney*

Mark Steffensen, *Vice Chair, Vice President and Counsel, Morgan Stanley & Co.*

Government Operations Committee

Kevin Caffrey, *Chair, Executive Director, Morgan Stanley & Co.*

Bryan Burns, *Vice Chair, Managing Director, Greenwich Capital Markets*

MBS/ABS Executive Committee

Jeffrey Perlowitz, *Chair, Managing Director, Salomon Smith Barney*

Kevin Finnerty, *Vice Chair, Managing Director, JP Morgan Chase & Co.*

MBS Operations Committee

Frank Malarkey, *Chair, Director, Credit Suisse First Boston*

Robert McLoughlin, *Vice Chair, Vice President, Goldman Sachs & Co.*

Risk Management Steering Committee

Maureen Miskovic, *Co-Chair, Managing Director, Lehman Brothers Inc.*

Steven Allen, *Co-Chair, Managing Director, JP Morgan Chase & Co.*

Carl Adams, *Co-Chair, Executive Consultant, International Monetary Fund*

Michael Alix, *Co-Chair, Senior Managing Director, Bear Stearns & Co., Inc.*

Operations Council

Laura LoCosa, *Chair, Managing Director, Morgan Stanley & Co.*

Kenneth Librot, *Vice Chair, Senior Managing Director, Bear Stearns & Co., Inc.*

Business Continuity Management Council

Steven Bernstein, *Chair, Head of Business Continuity, Citigroup*

Micah Green, President

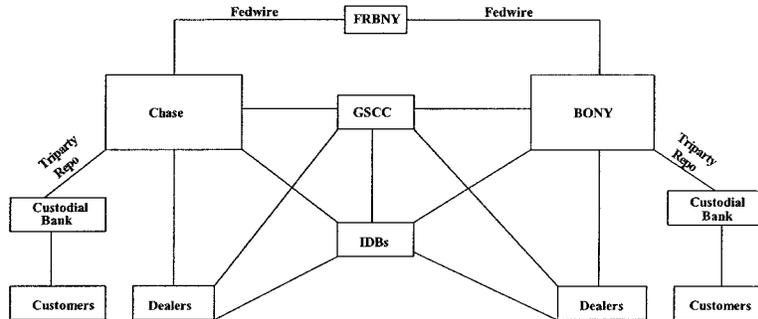
Paul Saltzman, *Executive Vice President and General Counsel*

Attachments

- Appendix A - Analysis of the Current Government Securities Clearance System
- Appendix B - Analysis of the Limited Purpose Bank Approach
- Appendix C - Analysis of the Old Euroclear Model
- Appendix D - Analysis of Enhancing the Federal Reserve System
- Appendix E - List of Task Force Members

Appendix A

Analysis of the Current Government Securities Clearance System



As mentioned in our letter (the "Comment Letter"), we feel that, at least in the short term, the shortcomings inherent in the current system can and should be addressed by enhancing the current structure. The Association believes that the adequate level of intraday financing currently provided by the Clearing Banks and the difficulty the alternative structures may have in providing similar amounts of intraday financing argue strongly in favor of having the industry focus initially on addressing the risks inherent in the current system and not on fundamentally altering the existing clearance and settlement architecture.

1. The Current Government Clearance and Settlement System Allows For a High Level of Liquidity in the Government Securities Markets By Providing an Adequate Amount of Intraday Financing to Dealers.

In addition to clearing and settling government securities, the Clearing Banks provide custodial and tri-party repo services to dealers. Both of these services give rise to Clearing Bank extensions of intraday financing to the dealers. In particular, such intraday financing may involve the Clearing Banks extending intraday credit by accessing DOD from the FRB NY and passing along some amount of that credit to the dealers.⁴² The Clearing Banks provide such intraday credit to the dealers on both an unsecured and secured basis. The lending of securities intraday and the provision of secured and unsecured credit is determined by the Clearing Banks based on a review of such dealer's creditworthiness and

⁴² As described in greater detail in our Comment Letter, the Board's recently revised PSR Policy allows for the extension of uncollateralized DOD by the Reserve Banks to depository institutions, up to the amount of their net debit caps. Depository institutions may draw upon DOD in excess of their caps, to an extent, by posting collateral acceptable to the Reserve Banks.

Appendix A
Interagency White Paper on Structural Change
August 19, 2002
Page 2

the availability of collateral. While standing lines of secured and unsecured intraday credit provided by the Clearing Banks are available to the dealers, the Clearing Banks in their discretion also provide for expansions of such credit lines depending on a dealer's past history with the Clearing Bank, the availability of additional collateral, and current potential exposure as a result of its settlement activities. This is a critical point, because it demonstrates that the flexibility the Clearing Banks have in extending credit to market-makers is based on their ability to view settlement activity and on their overall relationship to their dealer customers.

The Clearing Banks also provide intraday financing by allowing a dealer the use of securities on an intraday basis in connection with triparty repo services offered by the Clearing Banks. The securities sold (or "repoed") by a repo seller and cash used to purchase (or "reverse in") the repoed securities by a repo buyer are placed in a triparty custody account, usually with the dealer's Clearing Bank, which provides essential administrative functions, including the allocation of repoed securities in accordance with guidelines set by the repo buyer, and revaluing (or "marking-to-market") of securities in the triparty repo facility. On the day of a repo trade, by day's end, the triparty custodian transfers the repoed securities from the dealer's proprietary account to a custody account maintained by the triparty custodian on behalf of the repo buyer. The following morning, the triparty repo "unwinds", and in simultaneous transfers the repo securities are returned to the repo seller/dealer and the cash used to purchase such securities is returned to the repo buyer. The repo seller/dealer thereby has access to its securities during the day and can use them intraday to make deliveries in connection with its trading and financing activities (that is, up until the end of the day allocations). The triparty custodian through its management of the transfer process essentially finances the dealer's securities intraday. Under circumstances in which the repo buyer leaves the cash it used to purchase securities in its triparty account intraday (as could be the case in connection with a term repo transaction), no DOD is incurred by the triparty repo provider, or passed along to the repo seller. However, in cases where the repo buyer removes such cash from the triparty repo facility (as could be the case in connection with an overnight repo transaction or a transaction that is otherwise closing-out), the repo seller's overdrafts are not funded by such cash in the repo buyer's triparty account, and such triparty custodian/repo provider may incur a DOD from the FRBNY; if so, it would pass along such credit - and the attendant DOD fees it incurs - to the repo seller. Given that the cash used to purchase securities is often kept by the repo buyer at its account at the triparty bank, the unwind provides repo sellers with the inexpensive use of the repoed securities on an intraday basis.⁴³

In addition to the use of securities resulting from the unwind of a triparty repo, the Clearing Banks also occasionally provide dealers with intraday loans of other securities on their books to allow dealers to promptly make deliveries of securities.⁴⁴

⁴³ It should also be noted that the Clearing Banks also provide intraday financing through the operation of GSCC's GCF service. Much like triparty repo services offered within each Clearing Bank, the GCF service involves an "unwind" during which securities are returned to the repo seller and funds are returned to the repo buyer on an intraday basis.

⁴⁴ Under the PSR Policy, a dealer must make deliveries of Fedwire book-entry securities totaling more than \$50 million in \$50 million blocks, plus a "tail-piece" for the remaining amount. As such, intraday lending of securities is sometimes necessary for a dealer to promptly obtain a \$50 million block of a particular security for delivery.

Appendix A
 Interagency White Paper on Structural Change
 August 19, 2002
 Page 3

The Association believes that these liquidity enhancing services the Clearing Banks currently provide are absolutely essential to the smooth operation of the government securities clearance system, in times of relative normalcy, and particularly in times of market stress. As discussed in more detail in the following appendices, it is unclear if the alternative clearance systems set out in the White Paper would be able to provide adequate intraday financing to the government securities markets.⁴⁵

2. The Current Government Clearance and Settlement System Presents Operational Risk.

The events of September 11, 2001 were a painful reminder of the interdependent nature of the operations of critical service providers, and that there are certain operational risks inherent in the current government securities clearance and settlement system. They also underscored the fact that the proper functioning of our financial markets depend, in large part, upon the smooth functioning of the clearance and settlement infrastructure. Yet, as with any clearance and settlement system, some level of operational risk will always exist in each of the important entities in the current clearance and settlement structure – including the Clearing Banks, FRBNY, Fedwire, GSCC, MBSCC, the IDBs and the dealers – and the connections between such participants. As discussed in the White Paper, we agree that an operational problem at certain points in the current clearance system could cause serious disruptions throughout the entire system. For example, given its essential nature as a “bridge” for the delivery and receipt of funds and government securities, an interruption in Fedwire service would bring all inter-Clearing Bank clearance and settlement of government securities to a halt, and further prevent the Clearing Banks from accessing DOD from the FRBNY. Likewise, a disruption in services at one of the Clearing Banks would not only cause significant problems for the dealers clearing through such Clearing Bank, but also adversely affect dealers at the functioning Clearing Bank, given their inability to receive securities from dealers who clear through the affected Clearing Bank. Likewise, a disruption at GSCC could potentially be even more problematic than a failure at a Clearing Bank. Given GSCC’s integral role in today’s clearance and settlement process,⁴⁶ such disruption would raise the potential that its participants would not receive expected deliveries of cash and securities, and would not be able to determine their positions.

⁴⁵ In addition, as the Board acknowledges, one of its motives in the revision of its PSR Policy was to alleviate potential liquidity pressures that depository institutions may face in light of new payment system initiatives such as the Clearing House Interbank Payments System with intraday finality (CHIPS), the Continuous Linked Settlement (CLS) system, and the Federal Reserve’s settlement-day finality for automated clearing house (ACH) credit transactions. See, e.g., Interim Policy Statement with Request for Comment, Docket No. R-1107 at 4-6. Such initiatives highlight the importance of ensuring that any government securities clearance and settlement system continues to provide sufficient intraday financing.

⁴⁶ By comparing and matching trades between GSCC participants, offsetting such deliver and receive obligations to arrive at a net position, and becoming the counterparty for (or “novating”) such trades, GSCC plays an integral role in the reduction of settlement and credit risk in the current clearance system. By netting compared trades, GSCC reduces delivery and receive obligations to only one net deliver or receive obligation per dealer, per CUSIP, thereby reducing settlement risk. In addition, through novation, GSCC steps in as a highly creditworthy counterparty for such transactions, reducing the risk that a dealer would otherwise have with a lower-rated counterparty. While GSCC aides in the reduction of risk in the current government securities markets, additional “concentration” risks are presented by the integral role that GSCC plays in the clearance and settlement system, as described above.

Fortunately, many of the specific vulnerabilities that were highlighted in our system by the events of September 11 are capable of being addressed within the current structure and do not require a fundamental change in the system's current architecture. These "lessons learned" include the fact that business continuity planning at the Clearing Banks, GSCC, the dealers and the IDBs need to adequately take into account the potential for an area-wide disaster, such as the one experienced in lower Manhattan, and for the loss or inaccessibility of critical staff. Likewise, we all now more fully appreciate the possibility that a broad regional power or telecommunications failure could affect both the primary and the back-up sites of critical institutions especially if these sites are located in the same region. We believe the lesson has been learned that redundancy in communications systems is not necessarily achieved by making arrangements with multiple telecommunications providers because such communications lines may nevertheless still travel through a single potential point of failure.

The Association is therefore convinced that many of the operational risks inherent in the current system can and should be addressed through more coordinated industry-wide contingency planning and testing and the joint development by the industry and supervisory authorities of a model set of "sound practices" for business continuity planning.⁴⁷

3. The Current Government Clearance and Settlement System Presents Exit Risk.

The current system also presents certain exit risks due to the concentration of services in just two providers. Under the current system, exit risks generally stem from the fact that the Clearing Banks are two privately owned financial institutions that engage in a number of financial activities aside from clearance and settlement. Nevertheless, we believe that the exit risks present in the current system have been somewhat overstated in the White Paper. There is no question that, given the private nature of the Clearing Banks, one or both of the Clearing Banks may voluntarily exit from the clearance and settlement business. However, no safeguards or advance plan currently exists to prevent such voluntary exit. Although it is highly unlikely that either Clearing Bank would voluntarily exit the clearance and settlement business on short notice,⁴⁸ an orderly unwind would need to take place with sufficient time to transfer clearance and settlement operations to another facility.

⁴⁷ We feel that many of these significant vulnerabilities are already starting to be addressed through more robust business continuity planning and enhanced back-up facilities at the Clearing Banks and other key institutions. The Federal Reserve, the SEC, as well as other bank regulatory agencies have been jointly analyzing the events that followed the September 11 terrorist attacks to identify how the overall resilience of the financial system might be strengthened. As part of this effort, a "Financial Industry Summit on Business Continuity" was held at the Federal Reserve Bank of New York on February 26, 2002. In preparation for this summit, discussion notes were circulated that suggested that there may be benefits from developing more robust business continuity plans across the financial sector including rapid resumption of critical operations following the loss of one or more major operating locations or a wide-scale regional disruption. See Business Continuity Summit Staff Notes, Comment Letter, note 16 at 1. It is the Association's understanding that the regulatory agencies referenced above continue to explore the possibility of developing and issuing a model set of "sound practices" that would embrace certain business continuity objectives and identify the sorts of firms and activities those sound practices should cover. The Association fully supports these efforts.

⁴⁸ The events surrounding the voluntary exit of Security Pacific National Trust Company ("SecPac") from the business of providing government securities clearance and settlement services in the early 1990s offers considerable comfort that any such voluntary exit by one of the Clearing Banks would allow for an orderly migration of services. It is our understanding that SecPac continued to operate and provide clearance services for two years after Bank of America (which had acquired SecPac earlier) announced that it was

Potentially more problematic would be the involuntary exit by one of the Clearing Banks as a result, for example, of financial difficulties experienced by one of them or their criminal conviction. An example of an involuntary exit resulting from financial difficulties would be an insolvency brought on by activities of the Clearing Banks unrelated to clearance and settlement. In such an event, the Federal Deposit Insurance Corporation (FDIC), as receiver of the failed Clearing Bank, would need to determine how to resolve the failure in a manner that presents the lowest costs to its insured depositors.⁴⁹ It is unclear whether the FDIC would determine if the transfer of clearance functions from the failed Clearing Bank to a temporary clearance facility or "bridge bank" would be the least-costly resolution.⁵⁰ A de facto involuntary exit could also occur by an event – such as criminal conviction or guilty plea by one of the Clearing Banks – that would potentially cause such Clearing Bank's participants not to clear and settle through the Clearing Bank and to remove their assets from the Clearing Bank.⁵¹

4. The Exit and Operational Risks Present in the Current Government Clearance and Settlement System Should Be Addressed Without Structural Change.

The Association recommends that the industry and the Clearing Banks work with the Advisory Committee to develop a comprehensive transition plan, to obtain broader commitments from the Clearing Banks to regulatory authorities regarding adequate notice in the event of a voluntary exit, and to generally enhance existing private bilateral commercial assurances provided by the Clearing Banks. In addition, the Association recommends that the industry, working in conjunction with the Advisory Committee, study the involuntary exit risks present in the current system and work towards developing a comprehensive plan to mitigate such risks. In any event, the Association believes that in the near term the exit and operational risks present in the current system can best be addressed within the current structure of the system.

planning to exit the business, in order to facilitate the smooth, seamless conversions of its customers to other clearing banks.

⁴⁹ See 12 C.F.R. Section 360.1.

⁵⁰ The FDIC may still transfer clearance functions to a bridge bank, even if it is not the least-cost resolution, if the FDIC and the Board recommend otherwise, and if the Secretary of the Treasury invokes a "systemic-risk exception" by stating that such least-cost resolution would have an adverse impact on financial stability and economic conditions, and that the more costly resolution would help avoid such adverse effects. See, e.g., White Paper, at 4 and note 6. It is also somewhat unclear if the FDIC's new bridge bank would be able to provide sufficient intraday financing to the dealers given the undercapitalized condition of the failed institution. It seems likely that the Federal Reserve System would offer the bridge bank some reduced amount of DOD that it could utilize to extend intraday credit to the dealers for which it clears. However, the FDIC would probably have to offer some sort of guarantee to the FRBNY for any future losses it suffers in connection with extending DOD to the bridge bank.

⁵¹ Although the criminal conviction of a bank (or guilty plea) might not legally prohibit a depository institution from providing settlement services, we believe it is likely that many pension funds, municipalities and other buy-side firms that utilize a tri-party repo service would be either legally required under ERISA or otherwise inclined to move their funds and securities elsewhere.

Appendix A
Interagency White Paper on Structural Change
August 19, 2002
Page 6

Voluntary exit risk may be mitigated through a commitment by the Clearing Banks to maintain their clearance operations over a period of time. This commitment should take the form of private bilateral commercial assurances between each Clearing Bank and each of its dealer customers. In addition, the Clearing Banks should both make express commitments to the Federal Reserve and other supervisory authorities that they will not exit the business without giving adequate notice. Finally, as mentioned earlier, a comprehensive plan needs to be developed by the industry that provides general guidelines for an orderly transfer or unwind of the business in the event of either a voluntary or involuntary exit by the Clearing Banks.⁵²

While contractual provisions may help mitigate problems arising from a Clearing Bank's involuntary exit, commitments to regulatory authorities and private bilateral commercial assurances cannot, of course, mitigate involuntary exit risk itself. However, the Association believes that there are currently controls in place which help mitigate the risk of a Clearing Bank involuntarily exiting the clearance and settlement business as a result of financial difficulties. Such existing controls include risk-based capital requirements for the conduct of financial activities by both of the Clearing Banks and regulatory oversight by the Board of these and other banking and securities related activities. Specific to the clearance and settlement of securities, the Board's PSR Policy, for example, regulates and limits the extension of intraday credit in the form of DOD.⁵³

There are also additional steps that can be taken in the near future to address uncertainties regarding the involuntary exit of the Clearing Banks due to financial difficulties. An unwind plan (either as part of or apart from a contractual commitment by the Clearing Banks as discussed above), created in a time of relative calm, could set out steps for an industry consortium to agree, potentially along with one of the existing utilities, to a buyout of the insolvent Clearing Bank from the FDIC. Details regarding the continued provision of services could thereby be worked out in advance as part of a broader pre-packaged transfer plan or involuntary exit plan.

In addition to action by the industry, the relevant regulatory agencies could potentially help reduce the involuntary exit of the Clearing Banks as a result of financial difficulty, and further help mitigate issues arising were such an exit to occur. For example, there is currently an overlapping regulatory framework between the regulation of the Clearing Banks, which is conducted by the Board in conjunction with other bank regulators, and the regulation of GSCC, which is conducted solely by the Commission. While the Association does not believe that such entities should be regulated by both agencies, we do believe that an Advisory Committee, as discussed above, could help aid the coordination of the Agencies' treatment of such facilities. Uncertainty with regards to how the insolvency of a Clearing Bank would be treated by the FDIC⁵⁴ (and the amount of DOD available to a bridge bank)

⁵² As mentioned earlier, the orderly exit of SecPac from the government securities clearance business suggests that voluntary exit risk may be somewhat overstated in the White Paper. See supra note 7.

⁵³ See Comment Letter note 25 (describing PSR Policy).

⁵⁴ As noted earlier, it is unclear if the FDIC would determine that a transfer of the clearance functions from a failed Clearing Bank to a "bridge" bank would be the least-cost resolution to the liquidation of the Clearing Bank, or if the Secretary of the Treasury would invoke the systemic risk exception if the FDIC found that such transfer were not the least-cost resolution. See supra note 9.

Appendix A
Interagency White Paper on Structural Change
August 19, 2002
Page 7

could also be addressed by the FDIC, the Board, and the Treasury resolving this issue in advance.⁵⁵

Of course, as discussed earlier, a Clearing Bank may also face sustained operational difficulties. In this regard, the Association commends the Clearing Banks and GSCC for their continued efforts to mitigate operational risk through the implementation of robust contingency plans and their ongoing efforts to develop additional back-up data centers and more redundant telecommunications lines. We feel confident that these efforts, when coupled with the publication of model business continuity practices⁵⁶ and the development of a coordinated industry-wide approach to enhancing business continuity planning, will substantially reduce risk in the current system. These efforts should facilitate a new operating environment with enhanced redundancy, real-time backup capability and an adequate dispersal of staff and systems that is sufficient to ensure continued operations of key services through even sustained and severe disasters.

These plans include a review of the lines of communication between the Clearing Banks and other relevant entities to ensure that not only are such lines maintained by different service providers, but also are physically separate from one another to protect against a physical disruption at a certain point. We have been advised that many service providers are migrating toward using a split-operations (or active/active) model⁵⁷ for disaster recovery in lieu of the more traditional business continuity model that assumes the use of an "active" operating site with a corresponding backup site. Still others are using a combination of both approaches. The implementation of such real-time (or "hot") backup facilities should help ensure that there will be no interruption of service should a Clearing Bank's primary site experience operational difficulties. Plans to ensure that the correct personnel will be able to access and operate out of such backup facilities also continue to be reviewed and improved upon. Further initiatives such as the implementation of real-time trade matching (RTTM) at GSCC will ensure prompt matching and confirmation of transactions on a real-time basis to ensure that counterparties to transactions entered into prior to a disruption in the clearance

⁵⁵ In addition, given the unique role the Clearing Banks currently play in the government securities clearing system, it may be appropriate to revise certain regulations that currently apply to the Clearing Banks without regard to their special status. For example, the Board's current PSR Policy does not specifically recognize the special status that the Clearing Banks currently occupy in the clearance and settlement of government securities. As noted in our Comment Letter, an examination by an Advisory Committee should be conducted to determine whether certain aspects of the PSR Policy – such as the calculation of maximum daylight overdraft capacity – should apply in a different manner to the Clearing Banks' in comparison to other depository institutions. See Comment Letter, Section 4.2.

⁵⁶ See Business Continuity Summit Staff Notes, Comment Letter note 16 at 1; see also Financial Industry Summit on Business Continuity, Meeting Summary, Federal Reserve Bank of New York, Feb. 26, 2002 [hereinafter "Summit Meeting Summary"].

⁵⁷ In a split operations model, two or more active operating sites provide backup for one another with each site being capable of absorbing some or all of the work of another for an extended time period. However, implementing this approach can involve significant costs relating to maintaining excess capacity at each site. In contrast, a traditional model of business continuity involves an "active" operating site and a corresponding backup site. Under this approach, staff from the active site are expected to relocate to the backup site with the back-up site housing current backup copies of the relevant system hardware and software to support both the front office and the back-office clearance and settlement operations. Another shortcoming with this approach is that an effective backup site requires continuous testing.

Appendix A
 Interagency White Paper on Structural Change
 August 19, 2002
 Page 8

system will have a confirmed counterparty match for all trades up to the point of such disruption.⁵⁸

While the Association believes that the ongoing improvement of the clearance and settlement system will aid in reducing operational risk, we believe that more can and should be done. Along with creating a Data Repository as noted in the Comment Letter, another area in particular that should be addressed relates to the method of communication between the Clearing Banks and their participants. The standard messaging formats and data content differ at each of Chase and BONY. As such, in the event of a disruption of service, there is no ability to easily switch the clearance and settlement of government securities transactions from one Clearing Bank to the other or to a bridge facility.

One possible solution to this problem might be to use a structure similar to the sub-custodial account structure, which GSCC currently utilizes in its General Collateral Finance (GCF) service to allocate securities after the close of the Fedwire. Such a facility might be created between the Clearing Banks as a possible mechanism for "switching" positions between Clearing Banks in the event of an emergency. Another potential solution is the implementation of a standard or common communications protocol.⁵⁹ Although such a protocol would not automatically enable the switching of positions from one Clearing Bank to another,⁶⁰ it is a necessary first step in enabling such switch to ultimately take place. In addition, creating common protocols would allow the Clearing Banks to pool and share resources with regard to back-up data recovery capability and contingency plans, as described in our Comment Letter.⁶¹ Finally, another useful step in industry-wide contingency planning, might be to have each dealer and triparty customer as a precaution execute all necessary account agreements with the Clearing Bank it does not currently clear through.

As with addressing involuntary exit risk resulting from financial difficulties, the Association believes that the relevant regulatory agencies could also aid in the reduction of operational risk. For example, as part of their overall supervisory responsibilities, it is important that the Board and the other federal bank supervisory agencies encourage the development of

⁵⁸ See Government Securities Clearing Corporation Important Notice: "Interactive Messaging For Real-Time Trade Comparison to be Implemented November 17, 2000; Doc. GSCC085.00, October 26, 2000. See also Comment Letter, note 33.

⁵⁹ The Association is currently involved in the development of various communication protocols for the fixed-income markets, the most recent being our efforts to facilitate T+ 1 and straight through processing of fixed income transactions by helping develop a new standard messaging format. Information regarding the Association's various e-commerce initiatives, including the work of the Association's Online Bond Steering Committee and the protocols efforts of the joint BMA FIX Fixed Income Working Group, can be found at: <http://www.bondmarkets.com/e-comissues.shtml>.

⁶⁰ While a protocol would enable communication in a common "language" between the Clearing Banks, connectivity between the Clearing Banks would need to exist to enable the switching of positions. For example, if one of the Clearing Banks experienced operational difficulties, the necessary connectivity between the two banks would not be operating properly. In addition, the internal positions of the dealers at the affected Clearing Bank would need to be transferred to the remaining Clearing Bank or bridge facility.

⁶¹ A common protocol might have benefits beyond its effects in reducing operational risk. For example, to the extent that a common protocol facilitates customers' switching their business between the Clearing Banks, it is likely to increase competition and reduce prices.

Appendix A
Interagency White Paper on Structural Change
August 19, 2002
Page 9

industry-wide best practices for business continuity planning. Consistency among key institutions involved in the settlement of government securities transactions with respect to their contingency planning and disaster recovery capabilities is critical. Such guidance and coordination among peers would be particularly useful for the Clearing Banks and other institutions critical to the government securities clearance and settlement process since the services these institutions provide are so interdependent. In addition, given that the most efficient and effective manner of implementing contingency plans for the Clearing Banks is to ensure close coordination between the two, and a sharing of resources where appropriate, the Association believes that the Advisory Committee should play a central role in reducing operational risk in the current system. We envision the Advisory Committee facilitating coordination and cooperation between and among the Clearing Banks, GSCC and the Federal Reserve, coordination that might otherwise not take place given concerns about the applicability of antitrust laws to these conversations. Given that the clearance and settlement system has naturally evolved to today's duopoly⁶² of service providers in which the two Clearing Banks are the principal providers of clearance and settlement services for government securities, steps need to be taken to ensure that the antitrust laws do not prevent these institutions from working together to improve both of their disaster recovery capabilities.

In addition to the proposals set forth above with regard to reducing operational risk and financial vulnerability, concentration risk may also be addressed through providing incentives for additional financial institutions to provide clearance and settlement services. Such incentives may take the form of tax incentives, subsidies, or regulatory incentives. The Association believes that an Advisory Committee should review the possibility of an additional clearance and settlement facility entering the current clearance system, and determine what incentives may exist to induce additional clearance facilities to enter.

5. *The Private Nature of the Clearing Banks Provide Incentives for Innovation & Facilitate a Market Drive Fees Structure.*

Given the private commercial nature of the Clearing Banks, the Association believes natural market forces act on the Clearing Banks to ensure a level of responsiveness to the dealers' needs as customers even if as a practical matter it is costly for dealers to switch Clearing Banks. A dealer's ability to threaten to move its clearance operations from one Clearing Bank to another arguably provide sufficient incentives for the Clearing Banks to implement innovative practices and more robust contingency arrangements to prevent a loss of business. While some might argue that the LP Bank approach could facilitate greater innovation because dealers and other users could be directly represented on the LP Bank's board, we are not convinced that this would necessarily be the case. Whereas a Clearing Bank or other private service provider might have a sufficient profit incentive to pursue new products and approaches, the LP Bank's board might simply end up deadlocked on such issues and ultimately refrain from taking new initiatives. In short, we do not view the formation of an industry owned LP Bank as necessarily being a panacea for the industry's concerns about adequate innovation by service providers. Rather, we view the presence of customers on the LP Bank's board of directors as only marginally improving the responsiveness of the LP Bank to customer demands for innovation, efficiency and reduced costs.

⁶² See Comment Letter, note 30.

Moreover, current economic literature suggests that neither pure monopoly nor the textbook model of perfect competition necessarily provide the greatest incentives for innovation and technological change.⁶³ In fact, in some markets a certain amount of monopoly power that is manifested through structural concentration can be quite conducive to innovation especially in an industry undergoing rapid technological change.⁶⁴ On the other hand, very high concentrations of monopoly power rarely have a positive effect and are just as likely to retard progress by restricting the number of independent sources of new products and by dampening the incentive to gain market share through accelerated investment in research and development. In our case it seems that, while the two Clearing Banks actively competing with each other might have adequate incentives to innovate, it is nevertheless important to promote healthy competition between the Clearing Banks by further facilitating customers' ability to switch between them.

As noted above, the clearance and settlement of government securities involves "discretionary" fees, set by a clearance facility, and "non-discretionary" costs which are set by the Board and the FRBNY and passed along by the clearance facility to its participants. Given the private, "for-profit" nature of the Clearing Banks, we believe it would be inappropriate to comment on the "discretionary" fees that are charged, and equally inappropriate to implement any regulation that would dictate what such fees should be. However, the Association believes that increased competitive pressures with the implementation of common protocols (as discussed above), in addition to spurring innovation, will also allow market forces to act upon such discretionary fees in a positive manner.

The Association also notes that, under the current system, DOD fees are reduced given the netting effects of the Clearing Banks. While certain dealer participants are in an overdraft position, others are in a net positive position. As such, at the Clearing Bank level, the DOD drawn by the Clearing Bank is net of the positive and overdraft positions of its participants. This netting effect results in lowered DOD fees that the Clearing Bank passes along in the form of credits to its participants.⁶⁵

6. Conclusion

The Association believes that the current clearance and settlement system provides a stable and efficient structure for the clearance and settlement of government securities. In particular, such system provides crucial liquidity to the government securities market by providing adequate amounts of intraday financing to the dealer community. While risks exist in the current system, the Association believes that such risks are somewhat overstated in

⁶³ See F.M. Scherer and David Ross, *Industrial Market Structure and Economic Performance*, third ed. (Boston: Houghton Mifflin Company, 1990), p. 660) ("viewed in their entirety, the theory and evidence suggest a threshold concept of the most favorable climate for rapid technological change. A bit of monopoly power in the form of structural concentration is conducive to innovation, ... [since the risk of spillover — i.e., sharing the profits of innovation with other suppliers — is smaller than in an industry with many suppliers]").

⁶⁴ *Id.*

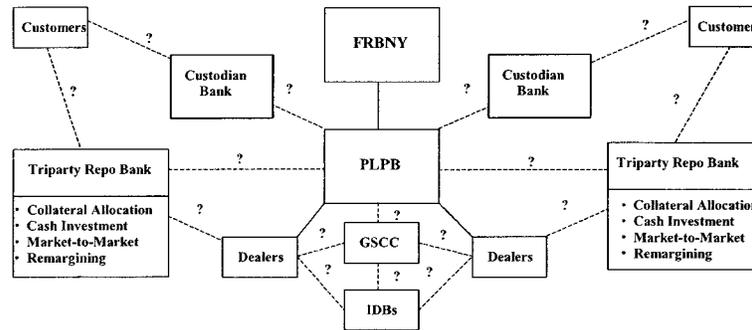
⁶⁵ As noted in our Comment Letter, the Association has previously supported the potential longer-term policy direction of the Board to potentially reduce DOD fees to the extent such DOD is collateralized. See Comment Letter, note 35.

Appendix A
Interagency White Paper on Structural Change
August 19, 2002
Page 11

the White Paper, and that ongoing and future initiatives could adequately address such risks while maintaining the structure of the current system. As discussed in detail in the remaining appendices, given concerns with the ability of an alternate system to provide necessary intraday financing and given the conversion costs of restructuring the current system, the Association believes that the majority of the industry's and the regulatory community's efforts should be focused on addressing the risks currently present without fundamentally altering the existing structure.

Appendix B

Analysis of the Private Limited Purpose Bank Approach



This alternative would involve the formation of a private limited purpose bank (the "LP Bank") that would provide core clearance and settlement services, and potentially other services such as triparty repo. As mentioned in our letter (the "Comment Letter"), the Association believes that this approach presents a number of potential benefits, including mitigating certain of the exit risks present in the current system. However, based on an initial review, it is not clear that this alternative could provide the needed liquidity for the clearance and settlement of the government securities market especially absent a bundling of triparty repo and core clearance services within the LP Bank itself. Nevertheless, the Association believes that the potential benefits this alternative provides makes it an approach that is worthy of further investigation.

1. Operational Risks and Exit Risks that Exist in the Current Clearance and Settlement Structure Could Potentially be Mitigated by Pursuing the Private Limited Bank Approach.

A number of operational risks and exit risks present in the current clearance and settlement system could be mitigated under this approach. If the LP Bank was formed as an industry owned utility,⁶⁶ it would not be subject to voluntary exit risk. Involuntary exit resulting from financial difficulties could also be mitigated by limiting the activities of the LP Bank to the clearance and settlement of government securities, thereby eliminating the possibility that the LP Bank could experience financial difficulties through the conduct of financial activities related or unrelated to clearance and settlement. Limitations on the LP Bank's financial activities would also theoretically limit the risk of other adverse events – such as criminal

⁶⁶ We assume for purposes of our analysis of this approach that the LP Bank would be organized, owned and governed by a representative group of industry participants as a public industry-owned utility. However, as we mention in our Comment Letter, an equally viable approach (the "Modified LP Bank Approach") may be for the Clearing Banks (perhaps together with certain custodial banks) to form and initially own the LP Bank as a private joint venture. See Comment Letter, Note 8. This approach is described in Section 6 of this appendix.

Appendix B
Interagency White Paper on Structural Change
August 19, 2002
Page 2

conviction – that could otherwise cause a de facto involuntary exit of a clearance facility.⁶⁷ In addition, as discussed below under Section 3, a strong corporate governance structure focused on mitigating the risks involved in clearance and settlement could also closely monitor the financial exposure of the LP Bank by setting and implementing stringent controls on intraday financing activities of the LP Bank.

While the LP Bank approach may potentially reduce a number of risks present in the current system, one risk that may potentially increase is concentration risk, since the clearance and settlement of government securities would be conducted in one location. The Association believes, however, that this risk can be significantly mitigated in the LP Bank approach in a number of different ways. In particular, a governance structure focused on ensuring the uninterrupted clearance and settlement of government securities would presumably implement robust contingency arrangements to protect against operational difficulties and to quickly address problems arising from such difficulties should they occur. Further, although the structure of the private limited purpose bank approach concentrates the clearance and settlement of government securities in one place, it may actually reduce operational risk by reducing the number of critical locations/interfaces that exist in the current system, where a disruption or failure could have a major adverse impact on the clearance and settlement of government securities generally.

2. It is Unclear Whether the Private Limited Purpose Bank Approach Would Provide Sufficient Intraday Financing to the Government Securities Markets.

Upon an initial review, it is unclear if the LP Bank would be able to provide sufficient intraday financing to ensure the continued liquidity of the government securities market. The Association's concerns revolve around the ability of a single entity to provide sufficient intraday financing, and the ability to "unbundle" triparty repo services from the provision of clearance and settlement services in general. The Association believes that, were this approach pursued, the LP Bank should provide both "core" clearance and settlement, as well as triparty repo services. However, even with such "bundling" of services, issues regarding the sufficient provision of intraday financing remain, as detailed below.

The ability of a single utility to provide sufficient intraday financing is of significant concern. For instance, it is our understanding that each Clearing Bank currently provides in excess of \$ 1 trillion⁶⁸ in intraday credit each day to the broader dealer community as part of its core clearance and settlement services. While it is likely that the need for Federal Reserve DOD would be substantially reduced if the LP Bank were the exclusive provider of clearance and settlement services to the dealers (as detailed below), it remains unclear if the LP Bank could obtain and provide sufficient intraday liquidity especially given the amount of exposure that the LP Bank and the Reserve Bank System would be subjected to.

⁶⁷ See Appendix A, note 10.

⁶⁸ Each Clearing Bank has a large number of smaller and regional dealers, in addition to the primary dealers, that clear through them, and this figure includes these clearance customers.

Appendix B
Interagency White Paper on Structural Change
August 19, 2002
Page 3

As detailed in our Comment Letter,⁶⁹ additional controls to mitigate the LP Bank's exposure to a clearance participant could include limitations on its provision of unsecured intraday credit or the elimination of any "subjective" discretion to extend such intraday credit. Such additional controls would not only mitigate the risk of loss to the LP Bank, but would also help prevent a risk of loss to the LP Bank's clearance participants assuming that they were subject to mutualization of loss for any costs incurred by the LP Bank. As an industry-owned utility, however, the LP Bank would also engage in a different risk/reward analysis than a purely private clearing bank when deciding whether to extend additional intraday credit to one of its dealer/customers. Because a user-owned utility typically returns any of its excess profits to its member/customers in the form of reduced fees or a special dividend, it does not have quite the same profit "reward" as one of the Clearing Banks. This difference may impact the LP Bank's behavior when providing intraday financing and make the reduction of such intraday financing under this approach more likely.

The imposition of stringent controls on intraday financing also gives rise to liquidity risk. While such controls may help mitigate the exposure of the LP Bank to its clearance participants, it may also restrict the provision of intraday financing to such an extent as to prevent the prompt delivery of funds and securities. For example, limitations on the amount of unsecured credit provided to clearance participants may provide insufficient liquidity to such clearance participants, resulting in delays in the delivery of funds and securities. Additional collateralization requirements may also reduce liquidity by forcing clearance participants to utilize government securities that would otherwise be available to settle trades to instead be used to obtain intraday credit. As noted in our Comment Letter, given the high level of liquidity in the government securities markets, and the reliance of dealers on such liquidity to make markets, a reduction in liquidity stemming from the imposition of more stringent intraday financing controls could directly impact the functioning of this market.

Assuming that the LP Bank were also to provide triparty repo services, it is similarly unclear if it would be able to provide the amount of intraday financing currently extended by the Clearing Banks through the "unwind" of triparty repo transactions. In addition to the large amount of credit that is extended each day to dealers as part of the general clearance and settlement of securities over Fedwire, each Clearing Bank also currently provides an average of \$ 400 - 500 billion in intraday financing of securities through the unwind of triparty repo transactions and related services.⁷⁰ Given the concerns stated above, it is unclear whether a single entity could appropriately manage such a high level of credit exposure on an intraday basis.

However, a strong argument can be made that, with the creation of a single entity, the demand for intraday DOD from the Federal Reserve may be very substantially reduced. First, with the LP Bank being the exclusive provider of government securities clearance and settlement services to the dealers, most inter-dealer transactions would occur intraday on the books of the LP Bank and not over Fedwire. As a result, there would be less need for the LP Bank to obtain DOD from the Federal Reserve System in connection with settling Fedwire transactions. Second, the need for dealers to obtain necessary intraday funding would be

⁶⁹ See Comment Letter, note 27.

⁷⁰ It should also be noted that the Clearing Banks also provide intraday financing through the operation of GSCC's GCF service.

Appendix B
Interagency White Paper on Structural Change
 August 19, 2002
 Page 4

reduced because funds transfer and DVP delivery of securities between separate Clearing Banks would substantially diminish. In other words, conducting transactions within the LP Bank would further reduce the amount of intraday credit being extended by the Federal Reserve System to the LP Bank. Finally, if triparty repo services were provided by the LP Bank, it is also possible that under the LP Bank approach, Federal Reserve and LP Bank DOD charges would not increase if repo buyers utilizing the LP Bank's triparty repo service left their funds in the LP Bank during the unwind of the triparty repo on an intraday basis. While it is unclear, the fact that all intra-dealer settlements in government securities would take place within the LP Bank, instead of over the Fedwire, may provide additional incentive for repo buyers to leave their funds at the LP Bank.⁷¹

A potential problem with the LP Bank approach is that the LP Bank may not have the same propensity to take on additional credit risk by providing intraday credit based on more subjective criteria. For instance, the Clearing Banks are currently in an advantageous position to manage the risks presented through their provision of clearance, settlement and triparty repo services given their broad financial relationship with their dealer/customers and their ability to obtain a security interest in a broad range of collateral that is unrelated to the clearance business. While it is likely that the LP Bank would be in a similar legal position as a creditor of a defaulting customer, Clearing Banks are able to be active liquidity providers to their customers, in part, because they have a well recognized contractual lien⁷² and a statutory right⁷³ to claim against a broader pool of financial assets already pledged to or held

⁷¹ Alternatively, the LP Bank might attempt to reduce intraday financing needs arising from triparty repo transactions by structuring their triparty repo services in a manner similar to the current Euroclear system. Euroclear offers triparty repo services to its members that are in certain ways substantially different from those offered by the Clearing Banks. Under the U.S. system, the Clearing Banks unwind the triparty repo transactions each morning by returning the cash to the repo buyer and the securities to the repo seller. As described above, this situation results in the Clearing Bank financing the repo buyer's securities position on an intraday basis. In contrast, under the current Euroclear model, triparty repos are not generally unwound each day. Instead, triparty customers rely on their ability to substitute securities intraday on the books of Euroclear and thereby gain full use of their securities. This results in Euroclear providing far less intraday financing resulting from its triparty repo services than is found in the current U.S. structure.

⁷² Clearing Banks generally rely on at least two separate legal bases for their claim to have successfully created and perfected a lien on the cash and securities contained in a broker/dealer's clearance accounts. First, the lien conveyed in the clearance agreement that it enters into with the dealer generally provides the Clearing Banks with certain rights in relation to assets kept by a dealer at the Clearing Bank. Clearance agreements typically give the Clearing Banks a broad lien on and right of set-off against all the customer's right, title and interest in securities, cash and other assets held in accounts at the Clearing Banks with the exception of client segregated accounts. This lien secures the customer's obligations to repay the Clearing Banks for any and all existing or future indebtedness or other obligations. Such agreements also commonly give the Clearing Banks broad remedies to enforce this interest, including the rights afforded a secured party under Article 9 of the Uniform Commercial Code ("UCC").

⁷³ The Clearing Banks, as securities intermediaries, typically obtain a perfected security interest in the securities held on their books under the relevant provisions of the UCC. Section 9-206 of Revised Article 9 of the UCC, for instance, provides that a security interest in a person's security entitlement automatically attaches and is automatically perfected in favor of a securities intermediary if (i) the person buys a financial asset through the securities intermediary in a transaction in which the person is obligated to pay the purchase price to the securities intermediary at the time of the purchase; and (ii) the securities intermediary credits the financial asset to the buyer's securities account before the buyer pays the securities intermediary. See 9-206 of the UCC; see also Note 4 in the Official Comment to Section 9-206, (indicating that a securities intermediary's security interest under this section is perfected by obtaining control over the asset and without further action.)

Appendix B
Interagency White Paper on Structural Change
August 19, 2002
Page 5

through the bank by a dealer. These liens provide the Clearing Banks with added security and allow the Clearing Banks added comfort when financing a repo seller's securities positions intraday during the triparty repo unwind. (However, the statutory security interest automatically obtained by the Clearing Bank under the UCC is more limited than the general rights conveyed in a clearance agreement.)⁷⁴ All in all, these rights provide the Clearing Banks with the ability to make subjective determinations on whether to expand a dealer's existing intraday credit lines.

Issues would also arise if the Bank were unable to provide triparty repo services. It is unclear whether a structure could exist where one could "unbundle" triparty repo from the clearance and settlement structure. By combining custodial and clearance and settlement services with triparty repo, the Clearing Banks have several means (some of which are detailed above) by which they prudently manage the risks that the provision of triparty repo services present. It is unclear if any potential triparty repo provider that had to rely exclusively on an agreement with a separate custodian/clearance entity in order to obtain a similar security interest in the dealer's securities and funds would have the same incentive to risk financing a dealer's positions intraday. The inability of such triparty repo provider to immediately and directly seize a dealer's securities that the triparty repo provider would finance during the unwind of the triparty repo could create a strong disincentive to provide such triparty services. In addition, by unbundling clearance and settlement and triparty repo, the triparty repo provider could not view the settlement activity of the repo seller intraday, further inhibiting such provider from determining a dealer's risk position and potential for failure. Further, unbundling triparty repo services from core clearance and settlement would likely encourage a repo buyer to remove its cash from the triparty repo facility during the unwind of such triparty repo. As discussed in Section 4 below, this may ultimately result in increased DOD fees.⁷⁵

Even assuming that triparty repo services could be unbundled from the clearance and settlement of government securities, other issues remain. For example, it is unclear if sufficient liquidity would be provided by several separate triparty repo providers during times of market stress. Even assuming that several triparty repo providers cumulatively would provide as much intraday financing of government securities as currently provided by the Clearing Banks through their triparty repo facilities, the willingness of a triparty repo bank to provide such liquidity in times of market stress without having a direct lien on the dealer's assets kept outside of such triparty repo facility is unclear. Such fragmentation of triparty repo services may therefore reduce liquidity during times of market stress where it may be

⁷⁴ In addition, it is our understanding that the Clearing Banks typically receive copies of the weekly focus reports that each dealer/customer submits to the NASD. They also are often granted the right to receive additional and more timely financial information if the credit rating of the dealer/customer falls below a certain level. When combined with the general lien and other security interests obtained by the Clearing Bank in the dealer's cash and securities under its control, the Clearing Banks, and to a lesser extent, the LP Bank, are arguably in a good position to evaluate and manage its exposure to the dealer resulting from a dealer's intraday overdraft position.

⁷⁵ One example of the unbundling of tri-party repo with clearance and settlement services was the previous experience of the Participants Trust Company (PTC) with providing this service. While PTC allowed financial institutions to provide triparty repo services to securities cleared through PTC, no financial institutions were willing to do so. However, PTC's inability to attract dealers may have had more to do with practical considerations (including the strength of existing relationships and a common desire to use only one triparty agent) than any fundamental flaw in PTC's service.

Appendix B
 Interagency White Paper on Structural Change
 August 19, 2002
 Page 6

most needed. Certain operational issues would also need to be addressed in connection with unbundling the triparty repo facility from the Bank; as the White Paper notes, a sub-custodial arrangement would need to be agreed upon between the triparty repo bank and the LP Bank for the transfer of funds and securities between the two. Such structure would increase operational risk by increasing the amount of connections needed for the operation of the clearance and settlement system.

3. A Strong Corporate Governance Structure May Offset the Lack of Competitive Pressures to Innovate under the Private Limited Bank Approach.

The Association believes that any potentially detrimental effects resulting from a lack of competition under the private limited purpose bank approach could possibly be addressed through the corporate governance structure of the LP Bank. In addition to the advantages set out above, the formation of the LP Bank as an industry owned utility would allow the industry to create a corporate governance structure that would allow for direct industry input and oversight of the LP Bank. This may help ensure that the LP Bank would continue to implement innovative practices, particularly with regard to risk management, regardless of the lack of competitive pressure.⁷⁶ However, it is unclear if such governance structure would present as great an incentive to innovate as the current system. The fact that dealers and other users were directly represented on the LP Bank's board might also simply lead to board deadlock and inaction on occasion, thereby preventing the investment in research and new software necessary to create new products and services.

4. Conversion Costs May Be Potentially High Under the Private Limited Bank Approach, While the Ability of such Approach to Reduce Fees Is Unclear.

The Association believes that, were the LP Bank approach to be implemented, an existing utility should be expanded to provide for the clearance and settlement of government securities. The costs of creating a central clearance facility may be limited if an existing utility – such as DTCC - were to be expanded to be utilized as such facility. Otherwise, while it is difficult to ascertain the exact amount of the costs involved in the formation of a clearance and settlement utility, such costs could potentially be very large.

Certain fees may be reduced under the private limited purpose bank approach. "Discretionary" transaction fees could potentially be reduced if the LP Bank was formed as a non-profit industry owned organization; presumably, such fees would cover the costs of ensuring a stable clearance and settlement system and would not be determined by profit motives. If securities were cleared and settled on the books of the LP Bank, the use of the Fedwire - and Fedwire fees - would also be significantly reduced.

It is possible that DOD fees may also be reduced. As noted in our Comment Letter, the DOD fees that the Clearing Banks currently pay are calculated on the basis of their net overdraft position, taking into account offsets between overdrafts in certain accounts with positive cash balances in others, thereby reducing DOD and related DOD fees. In this manner, a dealer pays a lower fee than it otherwise would if it were to incur DOD directly from the FRBNY

⁷⁶ See Goldberg & Kambhu, Comment Letter, note 37, at 5.

Appendix B
Interagency White Paper on Structural Change
August 19, 2002
Page 7

without being able to take advantage of the beneficial effects of offsetting balances at the Clearing Bank level. It is possible that such offsetting effects in the LP Bank would be even greater, resulting in lower DOD fees for its clearance members.⁷⁷

However, additional DOD fees may be assessed by triparty repo providers (assuming triparty repo services were unbundled from the LP Bank) if the funds which were "unwound" during the term of a triparty repo were removed from the triparty repo facility. While increased offset at the LP Bank may result in decreased DOD fees, the removal of funds from the triparty repo provider could result in substantial additional DOD fees. Assuming that triparty repo services were unbundled from the LP Bank, it is likely that the repo buyer would transfer the funds from the triparty repo provider to its account in the LP Bank, in order to utilize such funds to purchase securities. This would cause the repo seller to incur DOD at the triparty repo provider - and DOD fees.

Costs to the LP Bank could further be limited under a private limited purpose bank approach through the mutualization of loss in the event of a clearance participant's failure. By "mutualizing" the risk of loss, the costs incurred by the LP Bank resulting from a failure by a clearance participant would be shared by the remaining clearance participants. In the event that the LP Bank would incur a significant loss resulting from the failure of one of its clearance participants, such mutualization would help prevent a failure of the LP Bank itself by ensuring that its loss was mitigated or eliminated by the remaining participants, thereby reducing involuntary exit risk.

While mutualization of loss would mitigate the exposure of the LP Bank to loss resulting from the failure of one of its clearance participants, it is possible that it would increase certain other risks. For example, while mutualization of loss may help prevent the LP Bank's failure as a result of the failure of one of its clearance participants, such mutualization may cause financial difficulties for several of the remaining clearance participants responsible for reimbursing the LP Bank for losses it incurred. This risk would be especially acute in times of market stress, where certain clearance participants may already be exposed to financial difficulties. Reimbursing the LP Bank for its losses may exacerbate their current financial position, potentially causing additional failures.⁷⁸

5. Summary

While a number of concerns exist regarding the ability of this structure to provide necessary liquidity to the government clearance and settlement system, the Association believes that

⁷⁷ Note, however, that under the current system, the Clearing Banks are able to offset funds kept within their custody unrelated to the clearance and settlement of government securities (e.g. deposits, payments, etc., unrelated to the government securities markets) against overdrafts incurred by them in determining daily DOD. Assuming the Bank's activities would be limited to the clearance and settlement of government securities, such funds would not be present at the Bank, eliminating a source of offset that the Clearing Banks currently have to reduce their daily DOD position - and DOD fees.

⁷⁸ However, the LP Bank may institute other measures - such as clearing fund requirements - to mitigate the extent of loss incurred by each clearing member in the event of a failure by one clearing member. See Comment Letter at 16 and note 39.

Appendix B
 Interagency White Paper on Structural Change
 August 19, 2002
 Page 8

the potential benefits this alternative provides makes it worth investigating further. While concerns remain about the ability of a single entity to provide as much intraday financing as the government securities markets currently utilize, the Association believes that the potential risk mitigating effects of this approach justifies further investigation of this approach. Another approach, which may overcome certain obstacles of the LP Bank approach, is set out below.

6. Modified LP Bank Approach

Finally, the Association notes that the LP Bank does not necessarily have to be owned by industry participants and operate as a public utility. For instance, while the analysis we provide of the LP Bank approach assumes that the LP Bank would be formed as an industry owned utility, there are other ownership structures that are equally viable under this approach. One such approach is having the Clearing Banks jointly create and own an LP Bank (a "Private LP Bank") and thereby merge their back-office operations.⁷⁹

This approach would have a number of advantages with regards to the continued provision of adequate intraday financing and a reduction in the fees generally associated with clearance and settlement. First, under this approach, concerns about the adequate provision of intraday liquidity to the dealers might be minimized since the Private LP Bank would continue to have substantial Federal Reserve DOD capability assuming that each of the two Clearing Banks guaranteed any borrowing by the Private LP Bank. Second, as the exclusive provider of government securities clearance and settlement services to the dealers, most transactions would occur intraday on the books of the Private LP Bank and not over Fedwire, thereby reducing settlement risk for the Federal Reserve System and leading to greater efficiencies, reduced DOD charges and an overall reduction in the Fedwire transaction fees currently paid by the Clearing Banks on behalf of the dealers and other customers.⁸⁰ Third, since the provision of core clearance and settlement services would not be unbundled from triparty repo services, it is likely that the repo buyer would retain the cash used to purchase securities in the Private LP Bank after the unwind of a triparty repo. As such, dealers would have the Private LP Bank finance the intraday use of their securities without incurring DOD or DOD fees.⁸¹

Moreover, certain exit risks inherent in the current clearance and settlement architecture may also be mitigated under this approach. Voluntary exit risk would be substantially reduced, given that operations could continue despite the voluntary exit of one of the Clearing Banks.

⁷⁹ It is also conceivable that greater cooperation and coordination between the Clearing Banks, such as the creation of common messaging formats and a Data Repository, could facilitate the Clearing Banks decision to create a Private LP Bank by physically merging both Clearing Banks' government securities clearance and settlement services and their triparty repo businesses.

⁸⁰ This assumes full usage of this facility by the participating clearing banks for all of their Fedwire activity and a maximization of internal clearances within the Private LP Bank.

⁸¹ Unlike with an LP Bank formed as a common utility, the Private LP Bank might also have the ability to take on additional credit risk that was based on more subjective criteria.

Appendix B
Interagency White Paper on Structural Change
August 19, 2002
Page 9

Likewise, given that the Clearing Banks' ownership⁸² of the Private LP Bank would consist of owning shares in the jointly owned facility, problems arising from involuntary exit risk might be reduced since such shares could more readily be offered to another bank in the event one of the Clearing Banks were to become insolvent. In other words, this approach would make any long-term disruption in the provision of services less likely upon the voluntary or involuntary exit of one of the Clearing Banks. Finally, under this approach, both Clearing Banks would have sufficient incentive during the transition from the current system to continue to invest in new technology because they could profit (at least in the short term)⁸³ from any efficiencies and cost reductions that were ultimately realized.⁸⁴

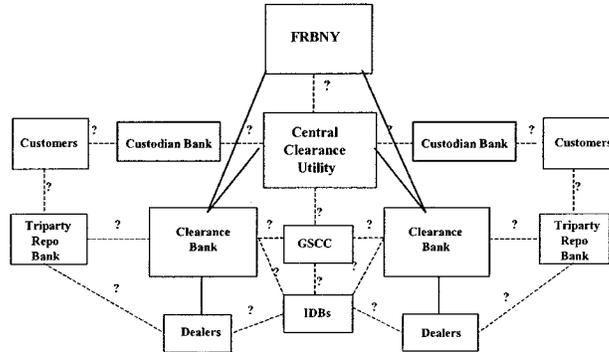
⁸² While the Private LP Bank might initially be owned by the Clearing Banks, this would not necessarily preclude the Private LP Bank from having a board of directors that included representatives from the dealer and investor communities.

⁸³ It is unclear whether the Private LP Bank should not also contain some ownership mechanism that facilitated the bank's ultimate evolution into a broader industry-owned utility once a sufficient period of time had elapsed and the Clearing Banks had fully realized an adequate return on their investment in the new entity.

⁸⁴ However, as with the LP Bank approach in general, one drawback with this approach is that it would lead to greater concentration of operational risk.

Appendix C

Analysis of the Old Euroclear Model



This alternative would involve the establishment of a central utility (the "Central Utility") that would enter into long-term service contracts with one or more clearing banks as suppliers of critical services, potentially including tri-party repo services. While this model may present some advantages over the current system, we believe that the industry's goals could also be more easily achieved within the existing structure through current or future industry initiatives, particularly given the potential costs of creating a Central Utility. We agree with the conclusion in the White Paper that "[t]his model's ability to address the vulnerabilities in the current system is mixed."⁸⁵

For reasons elaborated below, the Association believes that in order for this approach to provide any potential benefits over the current system, at least two clearing banks would need to provide credit and operational support to the Central Utility. Further, we believe that such clearing banks would also need to provide triparty repo services in order for this model to be successful, given the uncertainty as to whether triparty repo services could be unbundled from clearance and settlement, as noted under Appendix B, Section 2.

⁸⁵ See White Paper at 8.

APPENDIX C
INTERAGENCY WHITE PAPER RESPONSE
August 19, 2002
Page 2

1. The Ability of the Old Euroclear Model Approach to Provide Necessary Intraday Financing is Dependent on the Inclusion of More Than One Clearance Bank.

It is possible that this alternative would provide as much intraday liquidity as currently provided by the Clearing Banks if it did not substantively alter the current clearance structure. Under this approach, it is possible that the existing Clearing Banks would agree to enter into long-term service contracts with the Central Utility, and would thus continue to provide intraday financing through the provision of intraday credit and triparty repo services. However, assuming that the clearance and settlement of government securities would be separated from the clearance of other securities, intraday liquidity may still be adversely affected if clearance participants were unable to utilize non-government securities as collateral to obtain secured intraday financing from the Clearing Banks.

However, if a single bank were to provide operational and credit services (including triparty repo services) for the Central Utility, it seems unlikely that such bank would be able to provide sufficient intraday financing, for many of the same reasons discussed under the private limited bank approach in Appendix B. As discussed therein, it is unclear if a single entity could provide as much intraday financing as the Clearing Banks currently do, given the limitations on the amount of DOD it could access. Even assuming that a single entity had the capability of providing as much intraday financing as both Clearing Banks, the propriety of allowing a single entity to provide such financing is unclear, given the concentration of credit exposure that would result from the amount of intraday financing it alone would extend each day. In addition, under the old Euroclear approach, assuming such clearance facility were a private entity, significant concerns would arise about such entity to provide or refuse intraday financing at its sole discretion.

While concerns regarding the ability or propriety of a single entity to provide sufficient intraday financing may be alleviated by subjecting such entity to requirements set out by the Central Utility, such requirements may adversely impact liquidity. As discussed in Section 2 of Appendix B, while such requirements may help alleviate credit risk or assuage concerns regarding the discretion of the clearing entity, such requirements could also severely affect liquidity by, for example, preventing the clearing bank from making "subjective" extensions of intraday credit or imposing onerous collateralization requirements.

Finally, the Association believes that, under this alternative, any clearing bank providing services to the Central Utility should also provide triparty repo services. As discussed in detail in Section 2 of Appendix B, it is unclear whether triparty repo services could be successfully unbundled from clearance and settlement services. However, as noted above, if only one clearance and triparty repo facility exists under the Central Utility, it is unclear if a single entity would (or should) have the ability to provide as much intraday financing resulting from the unwind of a triparty repo transaction as currently provided by both Clearing Banks.

APPENDIX C
INTERAGENCY WHITE PAPER RESPONSE
 August 19, 2002
 Page 3

2. The Old Euroclear Model Alternative May Potentially Mitigate Certain Operational Risks and Exit Risks Present in the Current Clearance Structure.

A number of exit risks and operational risks may be mitigated under this approach, although such risks could be as adequately addressed within the current system. Voluntary exit risk could be mitigated through a contractual arrangement by the Central Utility with the clearing bank or banks whereby the banks are legally obligated to provide operational and credit support to the Central Utility for a specified time period. Operational risks could be mitigated in a manner similar to the mitigation of such risks under the private LP Bank approach, as discussed under Section 1 of Appendix B. Specifically, the Central Utility could impose robust contingency and back-up requirements on such banks to protect against a temporary cessation of services resulting from operational failures. Involuntary exit risk resulting from financial difficulties could also be mitigated by having the Central Utility limit its own financial activities. However, unless the Central Utility imposed similar limitations on the participant clearing bank or banks, this approach may not lead to a net reduction in involuntary exit risk in the overall system because the Central Utility is likely to rely heavily on such clearing banks for critical operational and credit support including triparty repo services.⁸⁶

While the old Euroclear approach may mitigate concentration risk through its dispersion of operational and credit risk through the use of multiple independent service providers, a level of concentration risk remains given the structure of this approach. Specifically, even if the Central Utility contracted with multiple clearing banks, concentration risk may still exist assuming that (as in the current structure) the exit by one clearing bank would materially affect the clearance and settlement of government securities. In addition, a temporary disruption by the Central Utility would presumably also materially impact the ability of the clearing banks to clear and settle government securities, further increasing concentration risk under this alternative.

Given the above analysis, the Association believes that, while this approach may potentially mitigate certain risks inherent in the current system, such risks may also be mitigated in a similar manner within the current clearance structure, as discussed in detail in Appendix A, Section 4. Addressing such risks in a similar manner within the existing system would provide the same risk mitigating benefits as under the old Euroclear model approach, while presenting the obvious advantage of eliminating any conversion costs that would be associated with such approach, as discussed below.

3. Conversion Costs May Be Potentially High Under the Old Euroclear Model Approach, Though Such Approach Could Reduce Fees.

As with the private limited purpose bank alternative, the Association believes that an existing utility should be expanded in order to create the Central Utility were the old Euroclear model alternative to be implemented. As noted in Appendix B, in all likelihood the costs involved in the formation of a new utility would be significant, whereas the expansion of an existing utility (such as DTC) would potentially limit such costs. Certain fees may be reduced under the old Euroclear model approach. Discretionary

⁸⁶ See White Paper at 14-15 (noting that "the utility would be exposed to the risk that a bank providing operational and credit services could involuntarily exit the business because of financial difficulties unrelated to clearing activities.")

APPENDIX C
INTERAGENCY WHITE PAPER RESPONSE
 August 19, 2002
 Page 4

fees, such as clearing bank fees, could be reduced under this approach if the Central Utility were able to negotiate a reduction of such fees with the clearing bank or banks. In a structure involving more than one clearing bank, Fedwire fees may also be significantly reduced if funds and securities were able to clear and settle within the Central Utility, instead of over the Fedwire. If only one clearing bank participated in this structure, Fedwire fees would be mitigated or eliminated assuming that the settlement of securities took place on the records of such clearing bank or the Central Utility. If the Central Utility were unable to clear and settle inter-clearing bank transactions, Fedwire fees would remain the same as under the current system, assuming a structure with more than one clearing bank.

As discussed in Appendix B, if the structure involved a single clearing bank, increased offsetting effects may reduce the amount of DOD needed by the clearance bank by netting positive and overdraft balances at the single clearing bank, thereby reducing the amount of DOD such bank would need to access. However, the extent to which DOD fees may ultimately be reduced would also be dependent upon the retention of funds in the clearing bank facility upon the unwind of a triparty repo, which in turn would likely depend upon whether triparty repo facilities were unbundled from the clearing bank, as discussed in detail in Appendix B. Regardless, the Association does not believe any potential benefit to be gained in relation to the reduction of DOD fees would justify the use of a single clearing bank, given the potential adverse impact on liquidity as discussed above, and in further detail in Appendix B, Section 2.

If the clearing bank or banks providing services to the Central Utility were private commercial institutions, the clearance participants would presumably not be subjected to mutualization of loss. However, assuming a structure that included more than one clearing bank subject to the Central Utility, it is unclear whether such approach would include the mutualization of loss at the clearing bank level. If so, upon the failure of one clearing bank, mutualization of loss at the clearing bank level could cause the remaining clearing bank or banks to encounter financial difficulties due to their obligations to share in any loss encountered by the Central Utility. If mutualization of loss was not present at the clearing bank level, the failure of a clearing bank or banks subject to the Central Utility could cause the Central Utility to undergo financial difficulties. In this manner, this approach would transfer to the Central Utility, rather than eliminate, problems arising from the involuntary exit of a participating clearing bank.

4. A Strong Corporate Governance Structure May Offset the Lack of Competitive Pressures to Innovate under the Old Euroclear Model Approach.

For the reasons discussed in Appendix B, Section 3 regarding the private limited purpose bank approach, the Association believes that the Central Utility should be formed as a publicly owned utility which would be governed by the industry. Industry governance and oversight of the Central Utility would help ensure continued innovation with regards to clearance and settlement functionality, provided the Central Utility was in a position to impose high standards on the clearing banks that supplied it with operational and credit support.⁸⁷

⁸⁷ However, as noted in Appendix B, Section 3, it is possible that such governance structure would not provide as great an incentive for innovation as private competitive pressures, given the possibility of disagreement and deadlock of the board of the Central Utility, which would lead to inaction.

APPENDIX C
INTERAGENCY WHITE PAPER RESPONSE
August 19, 2002
Page 5

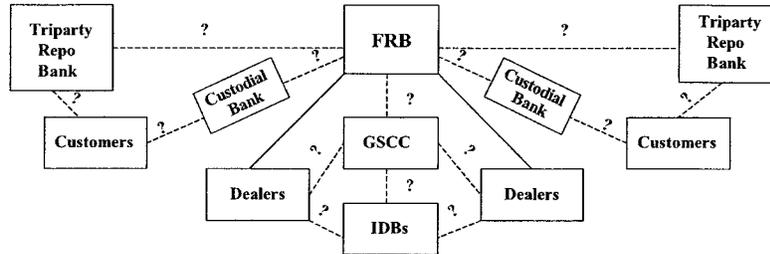
5. Conclusion

The Association is not yet convinced that this approach is as viable an option as improving the existing structure or moving to the private limited bank approach given: (i) the limited benefits such approach provides; (ii) the fact that many of the benefits it provides can also be achieved under the current structure; and (iii) the potentially significant costs involved in the creation of a Central Utility.

The benefits of this approach, as well as potential obstacles to its implementation, are similar in certain respects to that of the private limited purpose bank. Assuming at least two clearance facilities would participate under this approach, certain of the risks present in the current system could be mitigated while maintaining an adequate level of intraday financing. Further, certain costs may be reduced under this approach. However, it is unclear whether many of the benefits to be gained from this approach could not be accomplished by retaining and addressing the risks inherent in the current system, as discussed in detail in Appendix A, Section 1. If so, it is similarly unclear whether the expenditure of potentially significant costs in the creation of a Central Utility would be justified.

Appendix D

Analysis of Enhancing the Existing Federal Reserve System



As noted in our letter, this alternative envisages enhancing the Federal Reserve System in order to allow it to provide clearance and settlement services for government securities, as well as to potentially provide triparty repo services. While the Association believes that this approach may potentially eliminate many of the operational and exit risks inherent in the current system, we believe this approach to be the least viable of the alternatives set out in the White Paper. As discussed in detail below, our concerns stem mainly from questions regarding the ability and propriety of having the Federal Reserve act both as a provider of intraday financing to dealers as well as a direct or indirect regulator of such dealers.

7. A Number of Operational Risks and Exit Risks Could be Significantly Mitigated by Enhancing the Existing Federal Reserve System.

Voluntary exit risk, as well as involuntary exit risk resulting from financial difficulties, would effectively be eliminated under this approach. As the White Paper notes, "Federal Reserve services are not vulnerable to disruption because of financial difficulties."⁸⁸

As with any clearance and settlement system, operational risk would still exist under this approach. However, the Federal Reserve System certainly has more robust contingency and back-up arrangements than most non-governmental entities. In addition, given that the Federal Reserve System has considerably more resources available to it than to a non-governmental entity, the Federal Reserve would presumably be in the best position to mitigate against operational risk.

As the White Paper notes, a major risk inherent in enhancing the Federal Reserve System to provide clearance and settlement for government securities is moral hazard. The provision of intraday financing directly by the Federal Reserve System may give rise to less disciplined risk-taking by dealer and other market participants. While the validity of such concern is difficult to ascertain, given the robust risk controls implemented by each dealer currently, the Association believes that moral hazard would not significantly rise under this approach. In addition, as discussed in Section 2 below, the Association believes that the imposition by the

⁸⁸ See White Paper, at 10.

Appendix D
Interagency White Paper Response
August 19, 2002
Page 2

Federal Reserve of limitations on the amount of intraday liquidity provided by the Federal Reserve System would further reduce the risk of moral hazard.

2. The Federal Reserve System May Not Provide Sufficient Intraday Financing as a Clearance and Settlement Entity.

One of our main concerns with this approach is that it is unclear if it would provide sufficient intraday financing to maintain the level of liquidity currently present in the government securities market. Given the Agencies' recognition that the Federal Reserve System is not subject to financial difficulties, the limitations currently imposed on the Clearing Banks (and other depository institutions) on the maximum amount of DOD that may be extended could potentially be significantly expanded.

However, in all likelihood, the Federal Reserve System would limit the amount of intraday financing compared to the current system, by, for example, restricting the unsecured provision of DOD,⁸⁹ or eliminating subjective determinations to expand such forms of intraday credit. As mentioned above in Section 1, the Federal Reserve System would likely wish to limit credit risk to itself and to reduce the potential for moral hazard. In addition, unlike the Clearing Banks, the Federal Reserve System does not have any profit "reward" that it would reap in connection with the risks involved in their provision of intraday financing, further making the reduction of such intraday financing under this approach more likely. If the Federal Reserve System would not be as flexible as the Clearing Banks in the manner in which it would extend intraday credit, dealers may have insufficient access to needed funds, adversely impacting liquidity in the government securities markets.

The provision of additional forms of intraday credit – particularly "discretionary" forms of intraday credit – raises the related issue of whether the Federal Reserve System is an appropriate provider of additional forms of financing, particularly given their role as a regulator and their responsibility to avoid losses by the Federal Reserve System. In particular, many firms may be reluctant to access or request such additional forms of intraday credit, fearing that such request may raise increased scrutiny of a dealer's trading strategies and positions. Such reluctance may also apply to the Federal Reserve having direct knowledge of the positions in a dealer's securities and cash accounts; such direct access may adversely influence a dealer's trading strategy, causing such dealer to adopt overly conservative positions in the management of its portfolio, even if a more aggressive strategy may have been completely appropriate. Such adverse influence may adversely impact liquidity, leading to market distorting effects.

As discussed in detail under Appendix B, Section 2, the Association believes that the unbundling of triparty repo services from any clearance and settlement facility raises substantial issues with regards to risk management, as well as added operational concerns. As such, the Association believes that, were this approach to be implemented, the enhancement of the Federal Reserve System should include the provision of triparty repo services. As the White Paper acknowledges, however, were the Federal Reserve System to

⁸⁹ The extension of DOD under the most recent version of the PSR Policy may be unsecured up to the amount of a depository institution's net debit cap, which may be exceeded to an extent by pledging collateral. See Comment Letter, note 25.

Appendix D
Interagency White Paper Response
August 19, 2002
Page 3

provide triparty repo facilities, this would necessitate the creation and maintenance of a large number of accounts for non-depository institutions.⁹⁰ This would entail the provision of intraday (and potentially overnight) financing from the Federal Reserve System to these institutions, certain of which are not otherwise regulated. Given that some of these institutions are not as creditworthy as the dealers, the extensions of intraday or overnight credit to these institutions would likely entail increased credit risk to the Federal Reserve System and may in turn, require changes to the Federal Reserve Act itself. While such risk could be mitigated by requiring a pledge of liquid collateral, such risk mitigation controls raise the potential of reducing liquidity in the government securities markets by requiring financial institutions to utilize government securities as collateral, thereby limiting the amount of such securities available in the market.

3. While Conversion Costs May Potentially Be Low, Fees May Rise under the Enhanced Federal Reserve Approach.

We also believe that certain costs may rise under this approach, specifically DOD fees, as discussed below. In addition, given the fact that the dealers are not currently directly represented on the boards of the Reserve Banks, they would not be in a position to encourage a lowering of transactional fees.

Initial conversion costs could potentially be significantly lower than the other alternatives set out in the White Paper if the Federal Reserve were to fund the enhancement of the Federal Reserve System services in order to offer the clearance, settlement, intraday financing and triparty repo services of government securities to dealers. However, such costs would presumably be recouped over time by the Federal Reserve through the inclusion of such costs in transaction fees.

Assuming that the Federal Reserve would maintain the fee structure currently in place for the provision of DOD, such fees may rise significantly, given that the offset that currently takes place at the Clearing Bank level, as discussed under Appendix A, Section 1, would no longer be present. It is unclear if Fedwire transaction fees would decrease or increase, though given the fact that the Federal Reserve would not be motivated by profit concerns, it is possible that such fees may be reduced. However, such fees may remain comparable to transaction fees charged by the Clearing Banks, or may even increase, were the costs of enhancing the Federal Reserve System included in such fees, as noted above. If the Fedwire were to be utilized in the same manner as it is under the current system, presumably Fedwire fees would remain the same. Given the fact that the Federal Reserve System would not be susceptible to financial difficulties, the Association believes that no mutualization of loss would be necessary to protect it against potential exposure to the failure of a clearance participant.

⁹⁰ See [White Paper](#) at 11.

Appendix D
Interagency White Paper Response
August 19, 2002
Page 4

4. The Federal Reserve may not be Responsive to the Industry, Preventing the Implementation of Innovative Practices and Functionalities.

It is our view that the Federal Reserve would not be as responsive as a private institution or public utility to the industry's concerns or calls for innovation.⁹¹ Unlike a private commercial bank that is motivated by profit, or a public utility governed by the industry, the Federal Reserve System would not be strongly influenced by the industry with regards to the manner in which the clearance and settlement system should be conducted; how – and to what extent - intraday liquidity should be provided; and how risks in the system could best be mitigated. While the Association believes that such independence could in certain circumstances be beneficial, the risk of unresponsiveness may prevent the implementation of measures that would be needed to maintain a stable and liquid government securities clearance and settlement system.

5. Conclusion

Enhancing the Federal Reserve to provide clearance and settlement for government securities arguably would present the greatest reduction in the risks that currently exist in the clearance and settlement system. However, the ability of (and the propriety of) the Federal Reserve to extend sufficient intraday financing is unclear. In addition, while some costs may be reduced, others (such as DOD fees) may significantly increase. Another issue of potentially significant concern relates to the responsiveness by the Federal Reserve to the industry in relation to calls for a reduction in fees or the implementation of innovative practices. For these reasons, the Association believes that this alternative is the least viable of those presented in the White Paper.

⁹¹ While the Association commends the Board's and the FRBNY's continuing dialogue with the dealer community in connection with a broad range of issues, there have been past instances where such agencies have not been as responsive to the dealer community as the Association believes such agencies could have been. These instances include issues concerning the unilateral adjustment for principal and interest payments for securities subject to the Fedwire's repo tracking functionality, as well as issues concerning the inter-Clearing Bank transfer of securities after the close of Fedwire in connection with GSCC's GCF service.

Appendix E

a. INTERAGENCY WHITE PAPER TASK FORCE

<u>Name</u>	<u>Firm</u>
Mr. Frank DiMarco, <i>Task Force Chairman</i> <i>Managing Director</i>	Merrill Lynch & Co., Inc.
Mr. Andrew W. Alter <i>Managing Director & Counsel</i>	Salomon Smith Barney Incorporated
Mr. Thomas M. Brady	Bank of America NT & SA
Mr. Martin Brennan <i>Managing Director</i>	UBS Warburg
Mr. Shawn Brosko <i>Managing Director, Head of Operations</i>	Greenwich Capital Markets Inc.
Mr. John F. Coghlan <i>Managing Director</i>	Lehman Brothers Inc.
Mr. Adam Gilbert <i>Managing Director</i>	JP Morgan Chase & Co.
Mr. Joseph J. Grima <i>Director of Operations</i>	BrokerTec Global
Mr. Robert G. Knox <i>Senior Vice President</i>	Zions First National Bank
Mr. Kenneth E. Librot <i>Senior Managing Director</i>	Bear, Stearns & Co., Inc.
Ms. Laura E. LoCosa <i>Managing Director</i>	Morgan Stanley
Ms. Sibyl C. Peyer <i>VP & Associate General Counsel FICC</i>	Goldman Sachs & Co.
Mr. Brian E. Reilly <i>Managing Director</i>	BNP Paribas
Ms. Michelle Turner <i>Director</i>	Barclays Capital
Mr. Thomas J. Paul <i>Managing Director, Head of Fixed Income</i>	Deutsche Bank Securities Inc.
Mr. Andrew S. Carron – Consultant <i>Senior Vice President</i>	National Economic Research Consultants
Mr. Ralph Monda – Consultant	Oasis Inc.
Mr. William J. Santangelo - Consultant	

Appendix B



Securities Industry Association



October 21, 2002

Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, D.C. 20551
Re: Docket No. R-1128

Office of the Comptroller of the Currency
250 E Street, SW
Public Information Room
Mail Stop 1-5
Washington, D.C. 20219
Attention: Docket No. 02-13
Fax No. (202) 874-4448

Jonathan G. Katz
Secretary
Securities and Exchange Commission
450 5th Street NW
Washington, D.C. 20549-0609
Re: File No. S7-32-02

Elizabeth McCaul
Superintendent, New York State Banking Department
2 Rector St.
New York, NY 10006-1894

Re: Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System; Board Docket R-1128, OCC Docket 02-13, SEC File No. S7-32-02.

To whom it may concern:

The Securities Industry Association¹ and the Bond Market Association² (“the Associations”) are pleased to offer their comments in response to the White Paper on

¹ The Securities Industry Association brings together the shared interests of more than 600 securities firms to accomplish common goals. SIA member-firms (including investment banks, broker-dealers, and mutual fund companies) are active in all U.S. and foreign markets and in all phases of corporate and public finance. The U.S. securities industry manages the accounts of nearly 93 million investors directly and

Sound Practices to Strengthen the Resilience of the U.S. Financial System. The White Paper reflects the preliminary conclusions of the Board of Governors of the Federal Reserve System, the Comptroller of the Currency, the Securities and Exchange Commission, and the New York State Banking Department with respect to factors affecting the resilience of the critical markets and activities in the U.S. financial system in the event of a wide-scale regional disruption. The paper also offers the preliminary conclusions of the agencies with respect to a set of sound practices for core clearing and settlement organizations and other firms that play significant roles in critical financial markets. Finally, the paper also suggests an appropriate timetable for implementing these sound practices. Following the comment period, the agencies intend to publish a final version of the paper, which they intend to incorporate into supervisory expectations or other forms of guidance.

SUMMARY OF RECOMMENDATIONS

- Clarify that the purpose of the White Paper is to focus the attention of core and significant market participants on the need to engage in risk assessment exercises and have updated business continuity plans that address critical processes.
- Present any specific scenarios and sound practices as non-exclusive, non-binding examples of business continuity planning observed by the various agencies. Core and significant firms, in consultation with other stakeholders in the financial community, should have flexibility in developing the specifics of the scenarios and practices that make up an individual plan.
- Provide for another draft and comment period prior to final publication to ensure meaningful comment once certain issues and concepts are further clarified by the agencies.

indirectly through corporate, thrift, and pension plans. In the year 2001, the industry generated \$198 billion in U.S. revenue and \$358 billion in global revenues. Securities firms employ approximately 750,000 individuals in the United States. (More information about SIA is available on its home page: <http://www.sia.com>.)

² The Bond Market Association represents securities firms and banks that underwrite, distribute and trade in fixed income securities, both domestically and internationally, including all primary dealers recognized by the Federal Reserve Bank of New York. Association members collectively represent in excess of 95% of the initial distribution and secondary market trading of municipal bonds, corporate bonds, mortgage and other asset-backed securities, and other fixed-income securities and are also actively involved in the funding markets for such securities, including the repurchase and securities lending markets. This letter was drafted based on the input of the following Association committees: Interagency White Paper Response Task Force, Government Operations Committee, MBS Operations Committee, Business Continuity Management Council, Operations Council and the Board of Directors. Further information regarding the Association and its members and activities can be obtained at (www.bondmarkets.com)

GENERAL COMMENTS

We applaud the excellent cooperation exhibited by the agencies in soliciting the views of our member firms and preparing guidance for business continuity planning. The Associations strongly recommend that these cooperative efforts continue, particularly if the ultimate goal is publication of supervisory expectations or another form of guidance. Because firms create business continuity plans for the entire enterprise, it is critical that guidance be consistent for separately regulated entities of the same financial institution.

The broker-dealer community has also been working diligently, both as individual firms and collectively through the Associations, on the issue of business continuity planning. The tragic events of September 11 exposed vulnerabilities in business continuity plans, which firms undertook to address immediately. That resolve would have existed independent of regulatory pressure because of the strong competitive pressure that exists for firms to prepare for disruptions, including the demands of customers and counter-parties and other interdependent entities. The prodigious amount of work committed to planning is borne out by the results of a recently conducted SIA Business Continuity Planning ("BCP") Benchmarking Survey (to firms with 250 employees or more) designed to give BCP professionals in the financial sector a snapshot on what other firms were doing with their recovery programs. The survey found that additional reporting lines for business continuity had been added at the very top levels of the organizations and that the top priorities (of almost equal value) are people recovery, technology recovery (including telecommunications), and program assumptions. The survey also found that testing is an important priority. The survey also shows that, since September 11, personnel relocation changes have become further diversified with some firms moving further from their primary site, some diversifying their recovery location(s), some firms separating their people from technology, and some firms opting for other solutions. Also, the survey shows that, since September 11, all aspects of firms' BCP programs have gone through thorough review and many scenario assumptions have changed (i.e., from single building/small incident to multiple buildings/large area).

In December 2001, SIA formed a BCP Committee by incorporating a preexisting informal industry forum known as the Securities Industry Business Continuity Management Group. The Committee's mission is to:

- Provide a forum for securities firms, industry organizations, and service providers to share specific plans and business continuity information.
- Identify and develop business continuity plans and projects that have an industry-wide, rather than a firm-specific, focus.
- Provide a liaison between the securities industry and government legislators, regulators, and service providers, as well as to related industries such as telecommunications and power utilities.

Similarly, The Bond Market Association also formed a Business Continuity Management Council (“BCMC”), which serves as a standing advisory committee of their Board to advise on, and coordinate, their activities relating to fixed income business or industry utility disruptions and policy responses to the September 11th tragedy. The BCMC is composed of members of preexisting committees of The Bond Market Association, in addition to others with expertise in business continuity planning. The Bond Market Association is mindful of the need to ensure careful coordination with other industry groups that are working in this area, and will in particular provide input on an ongoing basis to SIA’s BCP Committee, as its work relates to fixed income issues.

In May 2002, the Associations responded to a similar proposed rule from the Board of Directors of the National Association of Securities Dealers, Inc. (“NASD”) concerning Business Continuity Plans and Emergency Contact Information.

In September 2002, the Associations responded to rule proposals of the New York Stock Exchange (“NYSE”) and the National Association of Securities Dealers (“NASD”) relating to business continuity and contingency planning. In their letter, the Associations expressed their support for the approach of requiring members to maintain auditable, updated plans that establish the firms’ procedures to be followed in the event of a significant disruption. Moreover, the NASD and the NYSE chose to identify the elements of continuity that plans should address – alternate physical location of firm and its employees, books and records back-up, alternate means of communication, etc. – rather than mandate what the plan ought to be. In fact, the theme that features prominently in both proposals is that plans should reflect the diverse nature of the member firm community and thus, the proposed rule ought to allow member firms to tailor plans to suit their, size, business, and structure.

Managing business continuity risk is not just a priority for financial institutions in managing a business; it is at the core of the services that they sell to the public. For this reason, financial institutions are especially qualified to successfully identify and manage this risk and therefore, ought to be given the opportunity to develop risk management practices as firms and as members of a responsible, interdependent financial community.

On the other hand, we respect the need of the agencies to be assured that critical financial markets and core and significant participants are studying the risks and planning accordingly. As the paper notes, the resilience of the financial system is only as strong as its weakest link and good planning will still require regulators to ensure that all of parties, including core and significant firms and critical financial (exchanges, utilities, etc.) and non-financial (telecommunications, government, etc.) entities participate in this effort. The Associations support identifying the processes and functions such as value transfers and pending transactions, as well as funding and posting of collateral that are deemed essential to recovery. The Associations also believe it is appropriate for the agencies to distinguish core and significant participants, although it will be just as important for the regulators to be sensitive to language that may be used to equate critical with capable, and thereby hurt the interests of many robust, smaller firms.

Beyond ensuring that core and significant firms have updated plans that address certain basic elements of continuity for critical processes elements of continuity in critical areas, we believe it is difficult if not impossible for the agencies to describe either the risks that an individual firm ought to consider or the means (or practices) that the firm ought to use to manage them. The Associations are concerned that some of the ideas presented in the White Paper go beyond illustrative examples and are intended to bind firms to a specific scenario and a specific plan or plan element. As the White Paper notes, firms feel strongly that "one size does not fit all." For example in specifying the base-line event for planning as a "wide-scale regional disruption," and suggesting that there exists an industry consensus around a sound practice of planning for separate labor pools, the White Paper makes questionable assumptions and conclusions that could limit the approaches that a firm might consider in light of its assessment of risk and the demands of its customers and the interdependent participants in its industry.

The Associations applaud the agencies receptivity to different approaches and ideas that is plainly evident in the document. Many of our comments stem from a concern that, because the agencies are also regulators, some of the more specific notions of guidance will give the ideas presented in this White Paper unintended legal weight and set standards. Moreover, many of the questions posed in the Request for Comment section seem aimed at the possibility of developing more specific guidance, which the Associations feel will apply a "one size fits all" approach for a diverse group of firms. The results of firms' planning efforts are always available for inspection by the appropriate examining authorities, who can determine whether the specific elements of any plan address the general goals and principles laid out by the agencies.

Finally, the agencies should evaluate the impact of the guidance on competition in low margin businesses like clearing. To the degree that the White Paper includes guidance that limits a core or significant firm's ability to implement cost-efficient solutions, some firms may decide not to continue in the business. This has important repercussions for end-user firms, the competitiveness of the business vis-a-vis foreign providers of these same services, and the concentration of risk within the industry.

SPECIFIC COMMENTS

Scenario

As described above, the Associations believe the establishment of a baseline scenario – "a wide scale regional disruption" - for continuity planning purposes is inadvisable. First, the scenario provided is extremely vague since a wide-scale regional disruption could potentially involve anything from a power outage to a direct nuclear strike. Second, the impact of each type of disruption would be different for different firms in the region and their responses would vary accordingly. Third, optimizing a plan for any one scenario could make the plan less effective in addressing other scenarios.

Some scenarios simply cannot be defended against due to consequences that are either unforeseeable, like certain extreme scenarios, or that are not within the control of the core/significant firm community, like problems experienced by infrastructure providers. Firms will base their decisions on the likelihood of the event and the cost of preparing the firm for it in light of the firm's overall resources. The cost of defending against some scenarios may be so high as to make it impossible for some organizations to continue to operate profitably. While core and significant firms take their roles seriously and have a natural interest in protecting and preserving a profitable business model, the ability to recover costs is a fundamental requirement of any business venture. To suggest a single scenario for which all firms ought to plan is to impose an unnecessary constraint on sound business and business continuity planning decisions.

Labor Pool

The Associations believe that "access to labor" is the appropriate issue that firm continuity plans ought to address. The White Paper suggests that there is industry consensus for a sound practice involving separate labor pools. Specifically, the paper states that out of region back-up locations should not be dependent on the same labor pool or infrastructure components used by the primary site, and their respective labor pools should not be both vulnerable to simultaneous evacuation or inaccessibility. Depending on the intended meaning of "separate" to describe a labor pool plan, our members would not agree that such a consensus exists.

The Associations believe that such guidance is unnecessarily limiting in that it suggests a single approach to addressing the issue of access to labor. The approach leaves the impression that only a stand-by labor pool would suffice. Creating a stand-by labor pool with the requisite expertise would be expensive. The Associations maintain that firms are in the best position to judge their "people risk" and so ought to have the maximum flexibility to manage this risk.

Limiting a firm's options to address the labor issue could in some instances create inconsistencies with governmental economic development programs and, in some cases, contractual agreements between firms and local authorities. Both civic planning and business continuity are important policy objectives that need not conflict if firms have sufficient flexibility to plan for access to labor.

Geographical Diversity

Clearly, geographical diversity of facilities is an important element of business continuity planning. However, The Associations do not believe that the White Paper should recommend a specific distance or a sound practice that specifies an "out of region" approach. Distance is a factor that will mean different things to different firms in different locations under different scenarios. Firms have already made and continue to make significant investments in alternative sites and data centers based on risk

assessments including costs and benefits. A prescriptive approach to distance in the White Paper would require changes to current plans that could result in a huge loss of this investment for many participants. Moreover, as previously mentioned, state and local laws and economic incentive plans are also important factors that may be inconsistent with some notions of geographical diversity.

The White Paper also notes that greater geographical diversity may be possible as a result of continued improvements in data transfer technology. The Associations understand the importance of back-up data to business continuity. However, the Associations believe that the emphasis on technology unfairly prioritizes available technology over other critical factors, like cost, that firms must weigh in planning for alternative locations. Singling out a factor for special consideration can have the effect of limiting the approaches that firms can use in addressing geographical diversity in its business continuity plan. The discussion of technology also tends to create unrealistic expectations for a timetable for the development and adoption of technology. A firm cannot predicate its business continuity plan on the promise of future advances in technology.

Rather than suggesting a specific approach to geographical diversity, the Associations recommend that the White Paper draw attention to the factors that should be considered when planning for geographical diversity, such as access to labor, water supply, transportation networks, and telecommunications and power infrastructure.

Timetable to Implement

To the degree that the White Paper produces specific guidance that requires firms to assess risk differently or consider new risk mitigation strategies, firms will have to expend significant resources to alter the plan they already have in place. Making strategy revisions is likely to take more than the 180 days suggested by the paper because business plans are typically drawn up a year in advance consistent with the annual budgeting cycle. The Associations recommend allowing one year to make these changes to the plan.

With respect to the actual implementation of planned changes, the Associations support the flexible language included in the White Paper that recommends firms make changes as soon as "reasonably practicable."

Recovery Time

The Associations believe that there should be a clear distinction in any guidance issued by the agencies between the concepts of recovery and resumption. The key goal of recovery ought to be ensuring that critical firms complete transactions and manage financial risk. Recovery consists of core clearing and settlement of cash positions and in-flight transactions by the end of the business day, however defined. Recovery and resumption is a two-step process. Core clearing and settlement organizations, including

value transfer networks, must be able to start business processes before critical markets begin the process of recovery. If the financial utilities are not able to recover, the other participants in the financial markets will not be able to recover in an orderly way.

The core clearing and settlement organizations must also be able to communicate that they are ready to begin processing prior to the running of the clock for recovery by the critical markets. The Associations believe that the financial utilities should be in a position to process transactions prior to the “end of day.” The Associations believe that any guidance should address the time that business operations can be re-started, not the time that recovery will be complete. Actual recovery time will vary depending on the time and nature of the disruption and the impact felt by an individual firm. Although hard targets should be avoided, a sufficient window for significant firms to *begin* the recovery process, after the core clearance and settlement and value transfer networks have resumed business operations, would be four hours.

The White Paper should make clear that resumption, or the ability to initiate new transactions, is a decision appropriately left to individual firms.

Core Firms /Significant Firms

The Associations believe the White Paper could better clarify the distinction between core firms and significant firms, referred to as “core clearing and settlement organizations” and “firms that play significant roles in critical financial markets.” The White Paper seems to distinguish the two based on involvement in clearance and settlement services. Yet some firms could conceivably fall into both categories for some functions or neither for other functions.

The Associations believe that it is appropriate to target guidance at firms whose role is critical to the continuity of the market and whose inability to perform critical functions would add systemic risk to the market. The Associations believe significant firms should be determined with reference to individual products. The methodology used for identifying significant firms ought to be clearly articulated by the agencies in order to provide adequate notice to affected firms. Furthermore, the methodology ought to be based on objective, material, publicly available data (i.e., volume), so that each firm can independently track its status. Finally, eligibility also ought to be determined according to historical, moving averages so that firms don’t abruptly change status. Once eligibility status is determined, the firm ought to have a reasonable time to develop or revise its plan and then to implement. To be consistent with the discussion above on the timetable to implement, newly eligible firms ought to have one year to make plan changes, and be subject to the “reasonably practicable” standard for actual plan implementation.

The agencies should also have the discretion to provide exemptions from critical firm status on a case-by-case basis.

Regulations/Laws

As we learned in the period following September 11, a flexible approach to regulation during times of great stress can be integral to limiting the eventual damage. Then, regulators had to determine whether the failure of certain firms and customers to comply with regulations applied on a daily basis was the result of a willful failure to comply or the unavailability of records necessary to determine compliance. In the case of financial reporting rules, otherwise healthy firms that were unable to document compliance could have been faced with contractual and/or regulatory default had applicable rules not been relaxed. Regulators need to know in advance which stress points their regulations directly impact and to be prepared to be flexible. Being flexible also means having a plan to gather the information needed to make a quick decision. The plan should address the key market participants to contact, the appropriate questions to ask, and the possible options for the regulators to take.

The Associations believe that the following categories of regulation may be appropriate for such planning on the part of the agencies:

- Timely announcements from regulators whether and to what extent a day will not be treated as a business day.
- Registration and location requirements applicable to foreign workers and foreign offices to allow firms an overseas option in their plans.
- Coordination with international regulators regarding any foreign regulation (i.e. data privacy) that could limit the ability of a firm to consider an overseas component in planning.
- Broad antitrust exemption authority to allay any concerns about the appropriateness of cooperative steps that will be necessary for recovery and resumption and permit firms to consider reciprocal arrangements with other firms as another option in their continuity planning.
- Specific regulations which present issues potentially impacting liquidity during an emergency situation include:
 - Rule 15c3-1 (capital charges for aged failed trades)
 - Rule 15c3-3 (collateral pledges, reserve accounts and affiliate status)
 - Rules 23A and 23B (inter-affiliate transfers of funds and extensions of credit)
 - Rule 431 (collection of margin)
 - Federal Reserve Risk-Based Capital Guidelines (maintaining required daily positive margin)
 - Regulatory Treatment of Business Locations Generally (various restrictions, including Regulation X, Section 23A, and Rule 15a-6, limiting the ability of firms to “pass the

book” on a temporary basis to allow functions to be assumed by a foreign affiliate).

Critical Markets/Products

We support identifying critical markets and products for additional guidance in the White Paper. The Associations agree with the recommendation to include foreign currency, commercial paper, government securities, corporate bonds and mortgage-backed securities, and would add cash equities, repos and reverse repo transactions. We believe that the criteria for identifying such products ought to be clearly defined in advance so that the agencies are not put in the position of making decisions about the relative importance of each product without the benefit of standards or context.

CONCLUSION

The Associations believe the White Paper can be most effective as a means of identifying the factors that core and significant firms need to address in business continuity planning without mandating what these plans ought to be. To the degree that specific scenarios and practices are included in the White Paper, they should be presented in context as part of a survey of non-binding, non-exclusive examples observed by the agencies. Finally, we believe that the interdependent nature of our industry requires that the agencies be vigilant with respect to the continuity planning of financial and non-financial entities, such as exchanges and power companies. The status of these interdependent entities will influence the success of the firms’ own efforts.

We hope that these comments are helpful and we look forward to a continuation of the constructive dialogue that has helped focus our members’ business continuity planning efforts. We would very much appreciate the opportunity to comment on a new draft of the White Paper once the agencies have a chance to clarify and refine some of the concepts it contains. Please feel free to contact Art Trager, Vice-President & Managing Director, Technology & Operations, SIA (212-618-0546; atrager@sia.com) or Rob Fry, Director of Fixed Income Operations, The Bond Market Association (212-440-9473; rfry@bondmarkets.com) with any additional questions you may have concerning these matters.

Very truly yours,

Jerry Klawitter
SIA Business Continuity
Planning Committee

Laura LoCosa
The Bond Market Association
Operations Council

cc: Board of Governors of the Federal Reserve System
Roger Ferguson, Vice Chairman

Securities and Exchange Commission
Division of Market Regulation
Annette L. Nazareth, Director
Robert Colby, Deputy Director

Federal Reserve Bank of New York
Laurence Sweet, Vice President

Depository Trust & Clearing Corporation
Dennis J. Dirks, President & C.O.O
Thomas F. Costa, President & C.O.O., GSCC
Jeffrey F. Ingber, Esq., Managing Director & General Counsel

Asset Managers Forum
Michael L. Wyne, Chair, Managing Director, Fischer, Francis, Trees &
Watts
Kenneth Juster, Director

Appendix C

369 Madison Avenue
New York, NY 10017-7111
Telephone 646.637.9200
Fax 646.637.9126
www.bondmarkets.com

1599 New York Avenue, NW
Washington, DC 20005-4711
Telephone 202.434.8400
Fax 202.434.8456

St. Michael's House
1 George Yard
London EC3V 9DH
Telephone 44.20.77 43 93 06
Fax 44.20.77 43 93 04



January 16, 2003

Roger Ferguson
Vice Chairman
Board of Governors of the Federal Reserve System
20th & C Street, Mail Stop 102
Washington, DC 20551-0001

Harvey L. Pitt
Chairman
Securities and Exchange Commission
450 Fifth Street NW
Washington, DC 20549-0001

William J. McDonough
President
The Federal Reserve Bank of New York
33 Liberty Street
New York, NY 10045-1003

Peter R. Fisher
Under Secretary for Domestic Finance
U.S. Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220-0002

Robert R. Glauber
Chairman and Chief Executive Officer
NASD, Inc.
1735 K Street NW
Washington, DC 20006-1516

Gentlemen:

The Bond Market Association respectfully wishes to bring to your attention a recently filed proposal by the Municipal Securities Rulemaking Board ("MSRB") to allow the MSRB to halt trading in municipal securities by declaring an "emergency." While this proposal directly affects only the municipal securities markets, we believe that the implications for other markets are significant.

The MSRB's unprecedented initiative to prohibit (and make unlawful) trading in one asset class of the over-the-counter ("OTC") bond markets raises serious and fundamental issues that have not been thoroughly vetted. Although we fully appreciate that this proposal is motivated by the best of intentions, we have serious concerns about both the authority, and propriety, of any governmental action that would serve as a precedent to "close" the OTC bond markets, which in times of stress need to provide liquidity that is critical to our nation's economy and banking system.

January 16, 2003

Page 2



A. The MSRB's Proposed Rule (the "Proposal")

We understand that the MSRB recently filed the Proposal with the Securities and Exchange Commission ("SEC"), and that it is awaiting publication in the Federal Register for a 30-day comment period. (A copy of the Proposal is attached.) If the Proposal is published for comment, we anticipate filing a detailed and comprehensive comment letter. Nevertheless, we thought a brief summary of our views would be appropriate.

The MSRB's proposal would add an interpretation to its general fair practices rule, Rule G-17, to provide that *if* the MSRB has declared an "emergency," any trading in municipal securities would violate Rule G-17. The proposed new interpretation sets out a broad and rather ill-defined range of circumstances under which the MSRB could declare an emergency. The MSRB also intends to reduce its quorum requirements when it considers making such a declaration. While the MSRB's Board of Directors comprises 15 members – bank dealers, securities firms and the public each have five representatives – a quorum for declaring an emergency would require only five members. Once a quorum is present, a majority vote could declare an emergency. Hence, a vote of three members of the MSRB's Board could conceivably close the municipal markets.

We also note that the Proposal appears to contradict the existing statutory regime for trading suspensions in two respects. First, section 12(k)(1)(B) of the Exchange Act, as amended in 1990, gives the SEC authority "summarily to suspend all trading on any national securities exchange or otherwise, *in securities other than exempted securities*, for a period not exceeding 90 calendar days." Since exempted securities were carved out from the trading-suspension authority, there is no basis for the MSRB (which itself was created under the direction of the SEC) to assume that power. Second, section 12(k)(1) provides that even an SEC order to suspend trading "shall not take effect unless the Commission notifies the President of its decision and the President notifies the Commission that the President does not disapprove of such decision." Further, section 12(k)(3) permits the President to lift a trading-suspension order, by directing that the order "shall not continue in effect." Given that even market closure orders that the SEC is clearly authorized by Congress to issue are ultimately subject to the President's authority, it would be anomalous in the extreme to give the MSRB the power to close the municipal market, which the SEC itself does not have and which is not subject to this additional presidential check.

January 16, 2003

Page 3



B. A Trading Halt in the OTC Markets Would Rarely, If Ever, Be Appropriate

The MSRB's proposal raises the question whether imposing a regulatory trading halt on a decentralized OTC market *ever* would be beneficial. We believe that the case has not been made that the grant of such authority is necessary or desirable. The municipal market, like other OTC bond markets, is highly decentralized, with participants dispersed across the country. Even in times of disruption, trading can occur on a bilateral basis so long as individual parties have the capacity to do so. The only possible central point of failure is the settlement and clearance system provided by the Depository Trust and Clearing Corporation ("DTCC"). But even if DTCC were to encounter difficulties, parties can decide whether to refrain from trading, or to extend the settlement period, or to make alternate settlement arrangements. Thus, even during an emergency, private sector participants should have the flexibility to decide whether to trade, subject to investor protection rules.

These points were well illustrated by the bond market's performance in the days following September 11, 2001. Market participants demonstrated an impressive ability to function in the crisis, by rapidly absorbing and assessing the facts and, where appropriate, making adjustments on a consensual and voluntary basis. After the attacks occurred, firms communicated with each other about their circumstances and capacities. Market participants collectively participated in this exchange of information and helped facilitate discussions about adjustments market participants might wish to consider. Through this process, market participants consensually agreed on voluntary recommendations in the days following September 11, including extended settlement periods for treasury securities (because that clearing system had experienced difficulties). This experience demonstrated the importance of allowing market participants the flexibility to adopt or reject temporary changes to business practices in time of emergency. Since September 11, the market's capacity for resilience has only strengthened, as firms have worked both individually and collectively to prepare for such contingencies.

Not only do we believe that imposing a regulatory trading halt is unnecessary, we also believe such a closing could be harmful. Whatever the circumstances, there is a benefit to economic and banking policy makers in allowing market participants to express views on credit and rates in a continuous way and to provide liquidity for investors who need it. To simply halt trading, even though some firms have the capacity to function, also could raise anti-competitive issues and reduce the incentive for firms to develop robust business continuity plans. Moreover, because most OTC markets today are interrelated and global, halting trading in one market could cause unexpected consequences in other

January 16, 2003

Page 4



markets or other parts of the world. Indeed, the notion of stopping all trading may itself be illusory, as derivatives and offshore trading may continue despite a ban on domestic trading – with the result that those subject to a governmental trading halt would be at a relative disadvantage.

Rather than prohibit trading, we respectfully suggest it would be better to address challenges raised by market emergencies in the OTC bond markets with firm-specific measures and targeted and enhanced investor protection and capital adequacy rules. Procedures could be developed, for example, to ensure that DTCC promptly notifies market participants of any difficulties it is experiencing, so that parties could decide what to do in light of potential problems or delays in settlement. Fair practice rules could be interpreted to provide that a firm should not enter into trades unless it reasonably believes it can complete them and that it should not knowingly misrepresent its capacity to execute or settle trades. Of course, existing rules already prohibit broker-dealers from charging excessive mark-ups. Other rules and procedures can be shaped to address any other specific problems that might occur during times of disruption.

In sum, as demonstrated by the events of September 11, market participants can respond to disruption in a fluid and flexible manner. Any additional regulation should be designed to support a nuanced and decentralized response to emergency conditions in the OTC markets. A regulatory trading halt is more likely to impede that process than assist it.

Particularly after September 11, regulators are appropriately focused on ensuring that markets continue to function as smoothly as possible during times of national emergency and that they have all the tools necessary to ensure that the public interest is served. We appreciate the efforts by the MSRB, SEC, and other regulators to undertake a thoughtful review of the existing regulatory system for this purpose. We do believe, however, that the instant Proposal by the MSRB raises complicated questions of law and public policy that need to be fully and deliberately vetted by the most senior of policy makers in our country in order to ensure that the public interest is best served by regulatory action in times of crisis. Further, because of the important interrelationships among market sectors, particularly in the fixed income arena, we think it is important that all agencies with an interest in the regulation of fixed income markets participate in this dialogue.

January 16, 2003
Page 5



On behalf of our membership, we would welcome the opportunity to work with all interested parties in continuing to address these important issues. Please feel free to contact Paul Saltzman, Executive Vice President and General Counsel, at 646.637.9214 or e-mail at psaltzman@bondmarkets.com, or John Ramsay, Senior Vice President and Regulatory Counsel, at 646.637.9230 or e-mail at jramsay@bondmarkets.com, if you have any questions or comments.

Respectfully,

Handwritten signature of Thomas Kalaris.

Thomas Kalaris
Chief Executive, Americas
Barclays Capital
Chair, Board of Directors
The Bond Market Association

Handwritten signature of Herbert (Bart) McDade.

Herbert (Bart) McDade
Managing Director and Head of Global Fixed Income
Lehman Brothers Inc.
Vice Chair, Board of Directors
The Bond Market Association

Handwritten signature of Micah Green.

Micah Green
President
The Bond Market Association

January 16, 2003
Page 6



cc: *Securities and Exchange Commission*
Cynthia A. Glassman, Commissioner
Harvey J. Goldschmid, Commissioner
Paul S. Atkins, Commissioner
Roel C. Campos, Commissioner
Annette L. Nazareth, Director, Division of Market Regulation
Robert L.D. Colby, Deputy Director, Division of Market Regulation
Alden S. Adkins, Associate Director, Division of Market Regulation

NASD
Mary L. Schapiro, Vice Chairman and President,
Regulatory Policy & Oversight

U. S. Department of the Treasury
Brian C. Roseboro, Asst. Secretary for Financial Markets
Timothy Bitsberger, Deputy Assistant Secretary for Federal Finance

Federal Reserve Board of Governors
Patrick M. Parkinson, Assistant Director

Federal Reserve Bank of New York
Dino Kos, Executive Vice President
Joyce Hansen, Deputy General Counsel and Senior Vice President

New York Stock Exchange
Edward A. Kwalwasser, Group Executive Vice President, Regulation

Commodity Futures Trading Commission
James E. Newsome, Chairman

Municipal Securities Rulemaking Board
Christopher A. Taylor, Executive Director
Diane G. Klinke, General Counsel

Depository Trust and Clearing Corporation
Jill M. Considine, Chairman and Chief Executive Officer
Dennis J. Dirks, President and Chief Operating Office

SECURITIES AND EXCHANGE COMMISSION
 (Release No. 34-_____; File No. SR-MSRB-2002-14)

December 20, 2002

Self-Regulatory Organizations; Municipal Securities Rulemaking Board; Notice of Filing of Proposed Rule Change Relating to Market Emergencies

Pursuant to Section 19(b)(1) of the Securities and Exchange Act of 1934 (the “Exchange Act”) and Rule 19b-4 thereunder,¹ notice is hereby given that on December 11, 2002, the Municipal Securities Rulemaking Board (“MSRB”) filed with the Securities and Exchange Commission (“the Commission”) a proposed rule change (File No. SR-MSRB-2002-14) (the “proposed rule change”) described in Items I, II, and III below, which Items have been prepared by the MSRB. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. SELF-REGULATORY ORGANIZATION’S STATEMENT OF THE TERMS OF SUBSTANCE OF THE PROPOSED RULE CHANGE

(a) The MSRB is filing a proposed rule change concerning market emergencies consisting of an Interpretation of its Rule G-17, on conduct of municipal securities activities and an amendment to its Rule A-4, on meetings of the Board.

The text of the proposed rule change follows. Italics indicate proposed additions and brackets denote proposed deletions.

Rule G-17. Conduct of Municipal Securities Activities

Interpretation of Rule G-17 – Effecting Transactions During Market Emergency

It is inconsistent with the principles of fair dealing embodied in Rule G-17 for a broker, dealer or municipal securities dealer to effect transactions in municipal securities

¹ 15 U.S.C. 78s(b)(1) and 17 CFR 240.19b-4 thereunder.

during a market emergency. For purposes of this interpretation, a market emergency is any situation causing a substantial failure in any of the systems necessary for clearance, settlement, confirmation, payment, or delivery of transactions in municipal securities or in other systems necessary for the prompt execution and consummation of municipal securities transactions or the fair and accurate pricing of municipal securities. In determining whether such a market emergency exists, a broker, dealer or municipal securities dealer shall rely upon the issuance of official announcements by the MSRB concerning market emergencies, which shall be issued after consultation with the Securities and Exchange Commission. Official announcements by the MSRB on market emergencies will be communicated to brokers, dealers and municipal securities dealers through news outlets commonly used in the municipal securities industry, by posting on the MSRB's World Wide Web site at www.msrb.org, and by transmittal of the announcement to the electronic mail addresses provided to the MSRB by brokers, dealers and municipal securities dealers under Rule G-40. Such official announcements will include information on the nature of the market emergency and affected systems, the nature and scope of transactions affected, and the status of the market emergency and its expected duration, if that is known.

Rule A-4. Meetings of the Board

(a) through (d) No change.

(e) Special Meetings on Market Emergencies. Notwithstanding anything in these rules to the contrary, the following procedures govern special meetings to act on market emergencies: (i) notice of a special telephone conference call meeting on a market emergency shall be sent to all Board members by the Executive Director, or in the

absence of the Executive Director, by his or her designee: (A) as soon as possible after credible information is received suggesting the existence of a market emergency, and (B) during the existence of a declared market emergency, within 24 hours of a request by any Board member; (ii) notice of a special meeting on a market emergency, including a description of the proposed Board action and instructions for joining the conference call, shall be given by telephone and by e-mail to all Board members; (iii) the Executive Director, or his or her designee, shall consult with the Commission on the emergency situation prior to a special meeting on a market emergency, if possible; (iv) the quorum requirement for a special meeting on a market emergency shall be five members and there shall be no requirement that at least one public representative, one broker-dealer representative and one bank representative be present; and (v) any action taken at such a meeting shall be by a majority vote of Board members attending the meeting and shall be limited to declaring a market emergency or ending a declared market emergency. For purposes of this paragraph (e), the meaning of the term "market emergency" shall be as defined in "Notice of Interpretation of Rule G-17 – Effecting Transactions During Market Emergency," dated _____.

II. SELF-REGULATORY ORGANIZATION'S STATEMENT OF THE PURPOSE OF, AND STATUTORY BASIS FOR, THE PROPOSED RULE CHANGE

In its filing with the Commission, the MSRB included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. The MSRB has prepared summaries, set forth in Section A, B, and C below, of the most significant aspects of such statements.

A. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

(1) Purpose

After the events of September 11, 2001, staff of the Commission and the MSRB met to discuss how the municipal securities market functioned in the aftermath of the attacks on the World Trade Center. On September 11, and in days following, the MSRB monitored the municipal securities market through its contacts with dealers, clearing corporations and information providers.

Although the effect on lower Manhattan was severe, because the municipal securities market is decentralized, the municipal securities market as a whole was not affected to the same degree as securities exchanges physically located near the disaster. On September 11, some trading in municipal securities occurred, albeit a very limited amount. Based on transactions reported to the MSRB's Transaction Reporting System, trade volume reached 8,244 trades by September 13 and 17,941 trades by September 17. On September 19 and 20 transaction volume reached 23,996 and 26,155 trades respectively. Prior to September 11, in a typical day, 27,000 transactions were processed.

Aside from dealer operations in Manhattan, in general, the infrastructure and systems necessary for processing transactions in the municipal securities market functioned in the days after September 11. Clearance and settlement systems for municipal securities transactions provided by Depository Trust and Clearing Corporation (DTCC) remained operational, although telecommunications problems in Manhattan did affect the ability of dealers in that area to exchange data with DTCC. The problems with clearing bank functions that disrupted the government securities market did not substantially affect the municipal securities market.

Despite the resilience of municipal securities market systems and infrastructure on September 11, there remains a concern about what might have happened if the situation had been different. Had systems or infrastructure critical to the municipal securities market been disabled by the disaster, no legal or regulatory mechanism existed to temporarily halt trading. For example, any problems with central clearance and settlement systems are of an immediate concern, since the accumulation of unsettled trades, particularly in a volatile or chaotic market, presents risks to all segments of the market. Commission staff accordingly have asked MSRB to consider rulemaking to provide a procedure for a trading halt should a market emergency disable critical market systems or infrastructure in the future.

The proposed rule change would provide such a procedure. Should a similar situation occur in the future, MSRB would review conditions in the market through its contacts with dealers, clearing agencies and vendors of critical services to the market just as it did after September 11. The proposed rule change, however, includes changes to the MSRB's administrative procedures in Rule A-4 allowing special MSRB telephone conference call Board meetings on market emergencies to occur without the normal notice requirement of seven days or the normal quorum requirement of two-thirds of the Board's members. The proposed rule change also includes a formal interpretation of Rule G-17, on fair practice, that would prohibit dealers from trading for the duration of a market emergency declared by the MSRB. These proposed rule changes thus provide a procedure for instituting a trading halt should a market emergency necessitate one in the future.

The proposed rule change specifically identifies the channels by which MSRB would make information known to municipal securities dealers in the event of a market emergency. It notes that this will be done through news outlets commonly used in the municipal securities industry, postings on the MSRB's web site and by transmitting announcements to the electronic mail addresses provided to the MSRB by dealers under Rule G-40, on electronic mail contacts. Having an announced, written procedure for dealer notification would add a level of preparedness if a market emergency actually occurs. Just as important, it provides dealers with clear direction on where to look if the situation is uncertain and questions exist about whether an emergency has been declared. This also will help dealers determine if any other emergency rulemaking is in effect. After September 11 there was some confusion among municipal securities dealers about whether the regular-way settlement cycle for municipal securities had been changed to T+5 from the T+3 cycle mandated under MSRB Rules G-12(b)(ii) and G-15(b)(ii). This apparently was the result of announcements made concerning transactions in government bonds. In monitoring clearance and settlement data after September 11, the MSRB observed that some dealers were, as a practice, submitting all of their regular-way trades with a T+5 settlement date. Among other problems, this caused trade-matching failures in the central comparison system for inter-dealer transactions. The notification procedure for market emergency declaration will help direct the attention of dealers in municipal securities to the MSRB for announcements on possible rule changes in the wake of an emergency and thus should help to avoid similar confusion in the future.²

² The proposed rule change addresses only the procedure for announcing trading halts. Should changes in existing MSRB rules be necessary during an emergency, these could be adopted by the MSRB and approved summarily by the Commission. Section 19(b)(3)(B) of the Exchange Act grants the Commission authority to approve proposed rule changes summarily when "it appears to

The proposed rule change's Interpretation of Rule G-17 follows a principle of securities law that a dealer must not "accept or execute any order for the purchase or sale of securities or induce or attempt to induce such purchase or sale if the dealer does not have the personnel and facilities to enable prompt execution and consummation the transactions."³ The MSRB believes that, where a substantial failure has occurred in the systems necessary for clearance, settlement, confirmation, payment or delivery of transactions in municipal securities, or in other systems necessary for the prompt execution and consummation of municipal securities transactions or the fair and accurate pricing of municipal securities, it may become necessary, for the overall protection of market participants, to halt trading by all dealers.⁴ Clearance and settlement systems are a particular concern because of counter-party risk that escalates when unsettled transactions grow during volatile or chaotic markets. Other situations possibly warranting a temporary halt in trading might include a massive failure of telecommunication systems, or the corruption of essential data used by the municipal securities industry (for example, through a computer virus).

Interpretation of Rule G-17

The proposed Interpretation of Rule G-17 has the following elements:

the Commission that such action is necessary for the protection of investors, the maintenance of fair and orderly markets, or the safeguarding of securities or funds."

³ See e.g., Release No. 34-8363 (July 29, 1968), 33 FR 11150 (August 7, 1968).

⁴ The scope of the proposed rule change does not include the issuance of "regulatory halts" similar to those issued by exchanges and other SROs to stop trading in a specific security pending the announcement of news, or to allow news to be absorbed by the market before trading continues. Since this situation would not constitute an emergency effecting essential systems and market infrastructure, it is not included within the definition of a market emergency.

- It is a violation of Rule G-17 for a dealer to continue to effect transactions in municipal securities during an MSRB-declared "market emergency."
- A "market emergency" for this purpose is defined as "a situation causing substantial failure in any of the systems necessary for clearance, settlement, confirmation, payment or delivery of transactions in municipal securities, or in other systems necessary for the prompt execution and consummation of municipal securities transactions or the fair and accurate pricing of municipal securities."
- Prior to acting on a market emergency, the MSRB will consult with the Commission.
- Official announcements by the MSRB on market emergencies will be communicated to dealers through news outlets commonly used in the municipal securities industry, by posting on the MSRB's World Wide Web site at www.msrb.org, and by transmittal of the announcement to the electronic mail addresses provided to the MSRB by dealers under Rule G-40.

Amendment to Rule A-4

Prior to making any decision on a specific market emergency, the MSRB will hold a special Board meeting to share information and discuss the situation. The MSRB's current procedure for holding special Board meetings is contained in Rule A-4. Among other provisions, the rule states that the Secretary of the Board will call special meetings at the request of the Chairman or at the written request of three or more members. Seven days written notice, signed by the Secretary of the Board (or three days notice if given or sent by telephone, e-mail or personal delivery), is required for special

meetings. The quorum for any Board meeting is two-thirds of the Board (normally ten members), with at least one securities firm representative, one bank dealer representative and one public member. Formal action requires an affirmative vote of the majority of the Board (normally eight members).

During a time of crisis, market participants would want to know fairly quickly whether trading is to be halted. The existing seven-day and three-day notice requirements for special Board meetings thus seem impractical. Moreover, establishing communication with at least ten Board members and securing eight affirmative votes also might present a problem, particularly if the emergency in question affects the infrastructure of one or more major financial centers and members cannot be reached. The proposed rule change would streamline the process specifically for market emergency meetings. The proposed amendment to Rule A-4 provides the following procedure:

- The Executive Director, or his or her designee, will schedule a special telephone conference call meeting on the possible declaration of a market emergency as quickly as possible after receipt of credible evidence that a market emergency exists.
 - At least one hour's advance notice of a special meeting on a market emergency will be sent to each Board member by telephone and e-mail.
 - The Executive Director, or his or her designee, will consult with the Commission prior to each special meeting if this is possible. (Note that consultation with Commission would be required by the interpretation of Rule G-17 governing trading halts. Thus, consultation with the Commission would have to occur prior
-

to any formal declaration of market emergency even if it does not occur prior to the meeting.)

- The quorum of ten members generally necessary for a Board meeting is replaced for special meetings on market emergencies with a quorum of five members. The general requirement that a member be present from each of the three statutory categories (securities firm, bank dealer, public member) does not apply.
- Board action at a meeting on a market emergency is limited to declaring a market emergency or ending a declared market emergency.
- A majority vote of members attending the meeting (not necessarily a majority of the Board) is required to take action.
- Once a market emergency has been declared, the Executive Director, or his or her designee, will schedule additional special conference call meetings on the market emergency within 24 hours after any request to do so by a Board member.

(2) Basis

The MSRB believes the proposed rule change is consistent with section 15(b)(2)(C) of the Exchange Act, which provides that the MSRB's rules:

... be designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade ... and to protect investors and the public interest

B. Self-regulatory Organization's Statement on Burden on Competition

The MSRB does not believe that the proposed rule change will impose any burden on competition in that it applies equally to all dealers in municipal securities.

C. Self-Regulatory Organization's Statement of Comments on the Proposed Rule Change Received from Member, Participants, or Others

Written comments were neither solicited nor received.

III. DATE OF EFFECTIVENESS OF THE PROPOSED RULE CHANGE AND TIMING FOR COMMISSION ACTION

Within 35 days of the date of publication of this notice in the Federal Register or within such longer period (i) as the Commission may designate up to 90 days of such date if it finds such longer period to be appropriate and publishes its reasons for so finding, or (ii) as to which the self-regulatory organization consents⁵, the Commission will:

- (A) by order approve such proposed rule change, or
- (B) institute proceedings to determine whether the proposed rule change should be disapproved.

IV. SOLICITATION OF COMMENTS

Interested persons are invited to submit written data, views, and arguments concerning the forgoing, including whether the proposed rule is consistent with the Exchange Act. Persons making written submission should file six copies thereof with the Secretary, Securities and Exchange Commission, 450 Fifth Street, NW, Washington, DC 20549-0609. Copies of the submissions, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in

⁵ The MSRB grants its consent to extend the comment period to 60 days.

accordance with the provisions of 5 U.S.C. 552, will be available for inspection and copying in the Commission's Public Reference Room. Copies of the filing will also be available for inspection and copying at the MSRB's principal offices. All submissions should refer to File No. SR-MSRB-2002-14 and should be submitted by [insert date 60 days from the date of publication].

For the SEC by the Division of Market Regulation, pursuant to delegated authority.⁶

Margaret H. McFarland
Deputy Secretary

⁶ 17 CFR 200.30-3(a)(12).



Testimony

of

**Richard G. Ketchum
President & Deputy Chairman
The NASDAQ Stock Market**

before the

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

on

**“Recovery and Renewal:
Protecting the Capital Markets Against Terrorism Post 9/11”**

February 12, 2003

Mr. Chairman and Members of the Subcommittee, I am Rick Ketchum, President and Deputy Chairman of The NASDAQ Stock Market. Thank you for providing me this opportunity to describe the steps NASDAQ has taken to ensure our business continuity in the event of another catastrophic event. NASDAQ is the world's largest electronic stock market. With approximately 3,700 companies, NASDAQ lists more companies and trades more shares per day than any other U.S. market. It is home to category-defining companies that are leaders across all areas of business including technology, retail, communications, financial services, media and biotechnology industries.

Because of the electronic nature of our market, it is important to note at the outset that at no time following the truly catastrophic disaster that occurred on September 11, 2001 were NASDAQ's systems inoperative. At the time of the 9/11 attacks, trading was suspended - but NASDAQ's systems and network continued to operate. Because our primary and backup technology centers are located outside Manhattan, and were therefore shielded from the damage to the downtown infrastructure, our primary concern related to our ability to connect with the firms that are active in NASDAQ and bring liquidity and order flow to our market place. In fact, NASDAQ continued to operate systems later than normal on 9/11 to allow firms manual access for reconciliation and mutual fund pricing and related

activities. NASDAQ's systems operated virtually continuously throughout the rest of the week to allow firms to test connectivity.

Following the 9/11 disaster, we worked constructively with the SEC, Treasury, Federal Reserve, NASD and the New York Stock Exchange (NYSE) as well as key member firms to resume trading on a coordinated basis as expeditiously as possible. That cooperation was an important factor in reopening the markets and restoring investor confidence in the markets. We at NASDAQ remain ready to cooperate again in that same spirit and we believe that American investors deserve nothing less. I am very proud of the efforts of so many talented people at NASDAQ who worked, tirelessly with so many others in the financial services community, to bring our markets back up on that Monday, 9/17, safely and without incident.

I will review, in a general way, our assessment of the potential challenges facing NASDAQ in the event of another crisis, explain NASDAQ's business continuity and disaster recovery plans, and describe our efforts to facilitate trading on an industry-wide basis should that prove necessary in the future.

I. Threat Assessment

Threats to NASDAQ could result from a variety of actions, intentional and unintentional, as well as domestic and foreign. Foreign threats may originate from

hostile nation-states, terrorist organizations, and other less organized groups that seek to degrade the U.S. critical infrastructure. Domestic threats range from groups seeking to destabilize the financial markets for political or criminal motives to hacker groups attacking highly visible organizations. Threats can come from outside the financial services community, from within our participants' organizations, and from within NASDAQ.

NASDAQ works continually to improve its understanding of the natural and artificial threats that exist in our critical national infrastructures, regional utilities, power sources, state transportation systems, and telecommunication systems and to translate that knowledge into our business continuity plans disaster recovery planning. NASDAQ also maintains close contact with the FBI, the Department of Homeland Security, and the SEC as well as state and local law enforcement so that critical intelligence information can be utilized to enhance physical security and gain insight into other threats such as electronic attacks and computer hacking.

While the events of September 11th did not fundamentally change NASDAQ's understanding of the potential range of threats to the financial services sector (whether acts of nature or man-made disasters), they amplified awareness of the potential reach that could be exerted by such threats. The events of 9/11 provided clarity and urgency to NASDAQ's business continuity and emergency/disaster recovery planning. In response to a potential increase in the

severity and likelihood of a threat to NASDAQ we have refined our personnel security strategy as it relates to access to critical information systems, including through increased background checks of all persons with access to our networks or systems to personnel checks and screening at our data centers.

II. Business Continuity/Disaster Recovery Planning

Keeping U.S. securities markets open is critical to the national and global economy. NASDAQ has implemented a fully developed business continuity/disaster recovery plan that will allow the continued trading of NASDAQ securities in the event that one of the NASDAQ data facilities is rendered inoperative. In short, we believe that disasters are managed not only by hardening potential points of failure, but also by building redundancies wherever possible into the entire trading network.

Geographic diversification of redundant facilities is a core component of NASDAQ's business continuity strategy. Our redundant data facilities are located hundreds of miles from one another in differing geologic and climactic zones so that the same natural event has a low likelihood of impacting both sites. NASDAQ also decreases its vulnerability by operating from separate utilities and local telecommunications services. This separation provides safety from regional events

such as weather, earthquakes, transportation shutdowns, data communication failures, disease, and other local problems that might harm the metropolitan areas.

NASDAQ's redundant trading facilities can accommodate comparable trading volumes. We staff both facilities on a 24-hour basis, and have a full complement of operations personnel on duty during the primary market period (9:30 to 4:30 ET) with each technical discipline that would be required to operate and maintain our trading environment.

NASDAQ's geographically decentralized network has several levels of redundancies, which are specifically designed to withstand catastrophic events. Virtually all firms are connected to NASDAQ through a set of several NASDAQ servers on their sites and in their backup centers. Each of the servers in the NASDAQ network is connected to two distinct NASDAQ connection centers.

There are more than 20 NASDAQ connection centers located throughout the United States – 4 in the NY metropolitan area. Each of these centers is connected to both our Primary and Backup data centers. Additionally, each of our critical connections is supported by numerous telecommunications vendors so as to offer resiliency against a systemic vendor failure.

NASDAQ enhances continuity of our telecommunication services by purchasing overlapping services from multiple suppliers that share no common infrastructures. Both local and national services providers facilitate local

connectivity to our facilities, and each has implemented its own isolated circuits. These local feeds enter our national network backbone at several locations and our national networks carry this diversity through to the participants' local telecommunications connections.

NASDAQ operates a variety of networks using both private (dedicated leased line), semi-private (shared leased line), and public (Internet) telecommunications systems and components. We have established baseline standards for network security, firewall, and intrusion detection, which are consistently exceeded in the design, implementation, and operation of our service networks. Core market products and services operate exclusively on secure custom-designed and private data networks, which are isolated from all other networks. We actively control vulnerabilities by maintaining patch levels on all systems/components and by thoroughly testing and managing all changes to our networks through a change control process.

At NASDAQ, our long-term strategy is to progressively "drive security down" into the lower layers of our infrastructure at each opportunity. Where we can, NASDAQ is focusing on providing access controls at the network and systems levels so that we can ensure that authenticated users are coming to NASDAQ only through their authorized servers and communication channels.

III. Industry-Wide Support

While we are confident that our systems design and contingency plans contain appropriate levels of redundancy, NASDAQ regularly works with our Member firms to enhance their backup capabilities. As a result of these ongoing efforts, I am sure that our equities markets are more resilient than they were on 9/11. NASDAQ has disaster recovery office space equipped with NASDAQ workstations and connectivity to NASDAQ that can be made available to participants who have temporarily lost access to or use of their trading facilities.

In addition to doing whatever we can to ensure continued operation of the markets, we continue to work with the SEC and the NYSE to develop a plan according to which NASDAQ and the NYSE can trade each others securities in the event of a disaster that rendered either market inoperable. Toward that end, NASDAQ has submitted to the SEC a proposal for a comprehensive Plan to facilitate the trading of securities listed on the NYSE should that need arise. The trigger for the implementation of this Plan is a catastrophic event that affects the NYSE's ability to operate for an extended period of time (two weeks or more). NASDAQ would implement the Plan only after consultation with and approval by the NYSE and the SEC.

Quoting and trading of NYSE securities by NASDAQ market makers would occur through NASDAQ's primary execution system, SuperMontage. NASDAQ market makers would self-register to trade the NYSE securities consistent with NASDAQ rules. Regional stock exchanges that are members of the NASDAQ unlisted trading privileges (UTP) plan and that are either linked to a NASDAQ quotation and trading system or report trades to the NASDAQ securities information processor (SIP) (or its successor) would be eligible to trade NYSE securities pursuant to the UTP. Post trade activity would take place through NASDAQ's Automated Confirmation Transaction (ACT) system. Clearing and settlement would occur through the Depository Trust Clearing Corporation. Market data dissemination (best bid, best offer, and last sale) would occur through NASDAQ's data dissemination facilities.

NASDAQ would, if necessary, trade all NYSE equity securities. It may be necessary to assign symbols to those securities that differ from those currently used by the NYSE, i.e., 4- or 5-character NASDAQ symbols. Transactions in NYSE listed securities would be monitored by NASDAQ MarketWatch and overseen by NASD Regulation.

NYSE securities would be subject to all the NASDAQ trading rules that apply to the quoting and trading of NASDAQ National Market stocks including, subject to SEC approval, the NASD Short Sale Rule. We would request that the

SEC exempt NYSE-listed securities from SEC Rules that govern normal trading of exchange-listed securities. NYSE-listed securities would be exempt from the requirements of the Consolidated Tape/Consolidated Quotation (CTA/CQ) and Intermarket Trading System Plans. Finally, NYSE-listed securities would be subject to the NASDAQ UTP Plan so that quotes and trades of NYSE securities would be printed on the NASDAQ tape.

It is important to emphasize that these plans, like the NYSE plans to trade some NASDAQ securities, are only a final layer of protection for the U. S. securities markets. The first line of defense for stock markets will always be their own back-up systems and the continued operation of each market has to be the first priority. Moreover, those back-up plans must result in no competitive advantage. As a result, NASDAQ would immediately cease operating this back-up system when the NYSE was ready to resume trading.

IV Conclusion

In the wake of 9/11, the U.S. financial industry demonstrated its resilience and resolve to maintain the most liquid and stable markets in the face of terrible challenges. Clearly NASDAQ's trading network has demonstrated its unique value as a part of this infrastructure. However, our work is not done. NASDAQ,

the government and the financial services industry will need to continue to work in concert to ensure that trading can resume following a catastrophic event.

The current legal and regulatory infrastructure that has resulted in the strongest, most resilient markets in the world is the result of far-sighted leadership over many years. Congress laid the foundation with the passage of the '33 Securities Act, the '34 Exchange Act and the '75 Act Amendments. However, the U.S. financial markets are not static; they will and should continue to evolve. It is in that light that I mention the importance of NASDAQ's application to be recognized as a national securities exchange, which has been pending at the SEC for over two years.

In addition to eliminating any potential conflict of interest that may arise from the current voting control by the NASD, as an exchange NASDAQ will shed a cumbersome board structure that could impede decision-making in a time of crisis management. Further, without such exchange status, NASDAQ is unable to raise needed equity capital to enhance systems and facilities on an ongoing basis and remain competitive with domestic and international competitors. Finally, as an exchange, NASDAQ will be able to more easily navigate regulatory obstacles to trading in securities listed on other markets in a crisis situation.

Thank you again for providing me this opportunity to describe the steps NASDAQ has taken to ensure our business continuity in the event of another catastrophic event. I would be happy to answer any questions.

TESTIMONY OF
Don Kittell
Executive Vice President
SECURITIES INDUSTRY ASSOCIATION

**“RECOVERY AND RENEWAL: PROTECTING THE CAPITAL MARKETS
AGAINST TERRORISM POST 9/11”**

BEFORE THE

Capital Markets, Insurance and Government Sponsored Enterprises

Subcommittee of the House Financial Services Committee

February 12, 2003

Subcommittee Chairman Baker and Members of the Committee:

I am Don Kittell, Executive Vice President of the Securities Industry Association.¹ I am pleased to appear before the Committee on behalf of SIA to testify about the business continuity planning (BCP) efforts of the securities industry. I applaud the Committee for its timely discussion of business continuity planning in a post 9/11 environment.

I am proud of the leadership role securities firms have taken through SIA to ensure our industry is better prepared to recover from future disasters. I especially applaud the work of the SIA Business Continuity Planning Committee to engage with securities exchanges, clearance and settlement organizations, service providers, financial services associations, state and local government

¹ The Securities Industry Association brings together the shared interests of more than 600 securities firms to accomplish common goals. SIA member-firms (including investment banks, broker-dealers, and mutual fund companies) are active in all U.S. and foreign markets and in all phases of corporate and public finance. Collectively they employ more than 495,000 individuals, representing 97 percent of total employment in securities brokers and dealers. The U.S. securities industry manages the accounts of nearly 93-million investors directly and indirectly through corporate, thrift, and pension plans. In 2001, the industry generated \$280 billion in U.S. revenue and \$383 billion in global revenues. (More information about SIA is available on its home page: www.sia.com.)

and federal regulators to develop a comprehensive approach toward business continuity planning.

Since 9/11, we have thought very differently about business continuity planning. The safety and security we all assumed we had just doesn't exist anymore. And disaster is no longer limited to a single building, single utility, or single market being down, but now includes the possibility of multiple buildings and entire geographic areas being devastated. Our industry is now in the midst of creating a systemic approach that covers a broader array of contingencies. And we must do all of this while we are managing in a tighter business environment. Indeed, we must find the most effective means of preserving the safety and security of our financial system without incurring overwhelming or unnecessary costs.

The War on Terrorism Is A National Priority

We have all had to absorb the implications of the war on terrorism – of 9/11, the war in Afghanistan, the instability of Pakistan, the insolvable conflict between the Israelis and the Palestinians, and now a potential war in Iraq and the uncertainty of its possible consequences in the Middle East and on oil prices. Perhaps the most significant outcome of the 9/11 attacks was the realization that the United States does not live in isolation, safe from terrorism in other parts of the world.

What has been the impact of that realization on the equity market?

- We now know that there is danger at home. Our assumption is that additional attacks will happen.
- Industry infrastructure is being dispersed to minimize single points of failure. Exchanges, clearance and settlement organizations, telecommunication companies, and clearing banks are investing in backup facilities.
- Following 9/11, disaster recovery became recognized as the responsibility of all business units, not just I/T or operations.
- Industry command centers are now in place and they are linked with other centers in municipal, state and federal government, as well as to other industry sectors such as telecommunications and transportation.

We cannot say we can defend against any and all attacks. But we can say we better understand the threat and have taken significant steps to prevent them from happening in the first place, and to recover from them once they do happen.

SIA Business Continuity Planning Effort

SIA Business Continuity Planning Committee (BCP Committee)

In December 2001, SIA formed a BCP Committee by incorporating a pre-existing, informal industry forum known as the Securities Industry Business Continuity Management Group. The Committee's mission is to:

- Provide a forum for securities firms, industry organizations, and service providers to share specific plans and business continuity information;
- Identify and develop business continuity plans and projects that have an industry-wide, rather than a firm-specific, focus; and,
- Provide a liaison between the securities industry and government legislators, regulators, and service providers, as well as to related industries such as telecommunications and power utilities.

The Committee also has seven subcommittees: Command Center; Exchange/Markets, Utilities & Service Providers; Industry Testing; Critical Infrastructure Planning & Urban Renewal; Best Practices; Insurance; and Catastrophic Events.

SIA BCP Committee Accomplishments

Through the seven subcommittees of the SIA BCP Committee, much has been accomplished, including:

- Issuing a lessons learned document, which is a collection of observations and experiences from those involved in ensuring business continuity (attachment 1);
- Producing Best Practices Guidelines (attachment 2), which recommend a Business Continuity Program, recovery strategies and recovery resources;
- Creating an industry command center with an established course of action plan. This center manages events impacting industry-wide operations. The command center links securities firms, exchanges and utilities, the New York City Office of Emergency Management and federal and state regulatory agencies. Physical and virtual facilities and communications links and contact lists are all in place. The first successful test of the command center was completed in May 2002;
- Developing a plan for industry testing (attachment 3) to confirm major institutions, exchanges and industry utilities could simultaneously activate work area recovery and data center recovery plans from alternate sites. This

initiative worked to increase the confidence level within the industry and in the investing public's view, to satisfy regulators that the industry can quickly recover from a widespread outage with minimal disruption to the financial markets;

- Presenting to the Lower Manhattan Development Corporation (attachment 4) recommendations on ensuring the financial community's concerns, especially as they relate to life safety, security, disaster preparedness and business continuity, are addressed in the redevelopment efforts of the World Trade Center site and surrounding areas; and,
- Providing the industry with education and awareness through the SIA website and conducting the first SIA BCP Conference this past October, with a strong program of public and private sector experts and approximately 350 attendees.

SIA BCP Committee Continuing Work

In addition, the SIA BCP Committee continues to work on further testing to confirm that major institutions, exchanges and industry utilities can simultaneously activate work area recovery and data center recovery plans from alternate sites. These efforts will increase the confidence level within the industry and in the investing public's view and to satisfy regulators that the industry can quickly recover from a widespread outage with minimal disruption to the financial markets. The committee is also expanding the scope of testing already underway via the SIA BCP Command Center, and developing and planning a course of action for specific catastrophic events using scenario planning. During this process the committee is working with major utility providers including telecommunications, power and water, and major industry vendors to determine and develop better ways to protect the industry. To that vein, the Committee is preparing to release a recently developed survey for service providers. (attachment 5, advanced copy).

Government and Private Sector Involvement

The SIA BCP Committee also continues to be an active participant in the newly formed Financial Services Sector Coordinating Council for critical infrastructure protection and homeland security (FSSCC). This private sector group was formed at the request of the US Treasury, which is chairing the Financial and Banking Information Infrastructure Committee (FBIIIC). The FBIIIC coordinates the protection, security and recovery efforts of 15 federal regulatory agencies.

The primary objective of FSSCC is to communicate between the private and federal regulatory sectors on business continuity issues. An organization established as the Financial Services Information Sharing and Analysis Center

(FS/ISAC) will assist FSSCC in its mission. The FS/ISAC is one of eight industry-sector ISACs established by presidential decision directive. The other seven sectors include government services, electric power, emergency services, oil and gas, water, telecommunications and transportation.

SIA Benchmark Survey

The prodigious amount of work committed to planning is borne out by the results of a recently conducted SIA Business Continuity Planning Benchmarking Survey. The survey was designed to give BCP professionals in the financial sector a snapshot on what other firms were doing with their recovery programs. The survey found that additional reporting lines for business continuity had been added at the very top levels of the organizations and that the top priorities are people recovery, technology recovery and program assumptions. The survey also found that testing is an important priority. The survey shows that since September 11, personnel relocation changes have become further diversified with some firms moving further from their primary site, some diversifying their recovery locations, some firms separating their people from technology, and some firms opting for other solutions. Also, the survey shows that since September 11, all aspects of firms' BCP programs have been thoroughly reviewed and many scenario assumptions have changed (i.e., from single building/small incident to multiple buildings/large area).

GAO Report: POTENTIAL TERRORIST ATTACKS, Additional Actions Needed to Better Prepare Critical Financial Market Participants

The SIA BCP Committee looks forward to a complete and thorough review of the newly released GAO study "Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants" (GAO 03-251). After a preliminary reading of the study, SIA agrees with the findings to identify strategies for recovery, determine the sound practices needed to implement these strategies, and identify the organizations that would conduct trading under these strategies. In the post 9/11 environment, the broker-dealer community has been working diligently, both as individual firms and collectively through the Associations, on the issue of business continuity planning, as suggested by the report. The tragic events of September 11 exposed vulnerabilities in business continuity plans, which firms undertook to address immediately. That resolve would have existed independent of regulatory pressure because of the strong commitment the securities industry has to its customers and the competitive pressure that exists for firms to prepare for disruptions, including the demands of customers and counter-parties and other interdependent entities. We feel strongly that a joint effort on the part of the industry and its regulators is a better approach to mitigate the risk involved for sound business practices. We stand by our comments to the agencies on business continuity and do not believe a "one size fits all" scenario is feasible. SIA and its BCP Committee look forward to continuing work with its regulators.

Joint SIA and TBMA Dialogue with Regulators

NYSE and NASD Proposed Rules

In September 2002, the Associations (SIA and TBMA) responded to rule proposals of the New York Stock Exchange (NYSE) and the National Association of Securities Dealers (NASD) relating to business continuity and contingency planning. In their letter, the Associations expressed their support for the approach of requiring members to maintain auditable, updated plans that established the firms' procedures to be followed in the event of a significant disruption. Moreover, the NASD and the NYSE chose to identify the elements of continuity that plans should address – alternate physical location of firm and its employees, books and records back-up, alternate means of communication, etc. – rather than mandate what the plan ought to be. In fact, the theme that features prominently in both proposals is that plans should reflect the diverse nature of the member-firm community and thus, the proposed rule ought to allow member firms to tailor plans to suit their, size, business, and structure.

Inter Agency White Paper

In October 2002, the SIA and the Bond Market Association (TBMA) again jointly responded to the proposed Interagency White Paper on "Sound Practices to Strengthen the Resilience of the U.S. Financial System." The associations applauded the excellent cooperation exhibited by the agencies in soliciting the views of our member firms and preparing guidance for business continuity planning. However, we strongly recommended that these cooperative efforts continue, particularly if the ultimate goal is publication of supervisory expectations or another form of guidance. Because firms create business continuity plans for the entire enterprise, it is critical that guidance be consistent for separately regulated entities of the same financial institution.

We respect the need of the agencies to be assured that critical financial markets and core and significant participants are studying the risks and planning accordingly. As the Interagency White Paper notes, the resilience of the financial system is only as strong as its weakest link and good planning will still require regulators to ensure that all parties, including core and significant firms and critical financial (exchanges, utilities, etc.) and non-financial (telecommunications, government, etc.) entities participate in this effort. The Associations support identifying the processes and functions such as value transfers and pending transactions, as well as funding and posting of collateral that are deemed essential to recovery. The Associations also believe it is appropriate for the agencies to distinguish core and significant participants, although it will be just as important for the regulators to be sensitive to language that may be used to equate critical with capable, and thereby hurt the interests of many robust, smaller firms.

Beyond ensuring that core and significant firms have updated plans that address certain basic elements of continuity for critical processes elements of continuity in critical areas, we believe it is difficult, if not impossible, for the agencies to describe either the risks that an individual firm ought to consider or the means (or practices) that the firm ought to use to manage them. The Associations are concerned that some of the ideas presented in the White Paper go beyond illustrative examples and are intended to bind firms to a specific scenario and a specific plan or plan element. As the White Paper notes, firms feel strongly that “one size does not fit all.” For example in specifying the base-line event for planning as a “wide-scale regional disruption,” and suggesting that there exists an industry consensus around a sound practice of planning for separate labor pools, the White Paper makes questionable assumptions and conclusions that could limit the approaches that a firm might consider in light of its assessment of risk and the demands of its customers and the interdependent participants in its industry.

Many of our comments stem from a concern that since the agencies involved are also regulators, some of the more specific recommendations contained in the White Paper could have unintended legal authority and set unnecessary standards. Moreover, many of the questions posed in the Request for Comment section seem aimed at the possibility of developing more specific guidance, which the Associations feel will apply a “one size fits all” approach for a diverse group of firms. The results of firms’ planning efforts are always available for inspection by the appropriate examining authorities, who can determine whether the specific elements of any plan address the general goals and principles laid out by the agencies.

Finally, the agencies should evaluate the impact of the guidance on competition in low-margin businesses like clearing. To the degree that the White Paper includes guidance that limits a core or significant firm’s ability to implement cost-efficient solutions, some firms may decide not to continue in the business. This has important repercussions for end-user firms, the competitiveness of the business vis-à-vis foreign providers of these same services, and the concentration of risk within the industry.

SIA believes the White Paper can be most effective as a means of identifying the factors that core and significant firms need to address in business continuity planning without mandating what these plans ought to be. To the degree that specific scenarios and practices are included in the White Paper, they should be presented in context as part of a survey of non-binding, non-exclusive examples observed by the agencies. Finally, we believe that the interdependent nature of our industry requires that the agencies be vigilant with respect to the continuity planning of financial and non-financial entities, such as exchanges and power companies. The status of these interdependent entities will influence the success of the firms’ own efforts.

CONCLUSION

The lessons we have learned from the terrorist attack on 9/11 will produce significant benefits to the industry. These lessons are hard. And there are legitimate concerns that some of the proposed reforms cause more problems than they solve. But, on balance, the benefits will be significant. And we will all be better off because of them.

Managing business continuity risk is not just a priority for financial institutions; it is at the core of the services that they sell to the public. For this reason, financial institutions are especially qualified to successfully identify and manage this risk.

Mr. Chairman, SIA appreciates the opportunity to share our views with you this afternoon. We hope that our comments are helpful and we look forward to a continuation of the constructive dialogue that has helped focus our members' business continuity planning efforts.

Thank you.

Mar-14-03 17:07 From:NYSE
 Robert G. Britz
 President & Co-Chief Operating Officer

2126568725

T-814 P.02/08 F-278

New York Stock Exchange, Inc.
 11 Wall Street
 New York, NY 10005

tel: 212-659-9057
 fax: 212-659-2303
 rbritz@nyse.com



March 12, 2003

The Honorable Richard Baker
 Chairman
 Subcommittee on Capital Markets, Insurance
 and Government Sponsored Enterprises
 2129 Rayburn House Office Building
 U.S. House of Representatives
 Washington, DC 20515

Dear Chairman Baker:

On behalf of the New York Stock Exchange ("NYSE" or "Exchange") and our Chairman, Richard A. Grasso, I am writing to respond to the three questions that you posed at the conclusion of the Wednesday, February 12, Capital Markets Subcommittee hearing.

1. What is the status of the NYSE's ability to trade unlisted (Nasdaq) stocks?

The NYSE has modified its systems to trade the top 250 Nasdaq stocks, which we understand comprise almost 80 percent of Nasdaq's average daily volume. We note that most of these stocks qualify under our rules for listing on the NYSE, which is to say that they are suitable for auction/agency trading on the NYSE. All NYSE systems have been modified and can support the four character symbols used by such unlisted stocks. Testing with the NYSE's member firms is underway and will conclude in the second quarter. The NYSE will schedule semi-annual production tests with all affected systems to enhance continued readiness to trade Nasdaq stocks in case of an emergency. We believe that our current capacity model and our continuing enhancements to our capacity are adequate. It should be noted that the NYSE's capacity is approximately five times our current average daily volume, which is approximately 1.45 billion shares. With the recent addition of capacity-on-demand from our technology vendors, our capacity is more than adequate to handle our message traffic as well as the additional message traffic for the top 250 Nasdaq securities.

2. What is the NYSE's reaction to the General Accounting Office's ("GAO") recommendation that the Securities and Exchange Commission's ("SEC") Automation Review Policy ("ARP") program require mandatory participation for all market participants?

Mar-14-03 17:07 From:NYSE

2126665725

T-814 P.03/08 F-278

The Honorable Richard Baker
Page 2
March 12, 2003

As the NYSE has always regarded the ARP process as consistent with our various other obligations (rule-based or otherwise) to the SEC, compliance with the process is never an issue. Although ARP provides a useful review program, on its own initiative, the NYSE builds complex trading applications, networks, systems infrastructure, etc. to ensure that its operating capability is robust, highly available and scaleable. It does so against stringent, self-imposed metrics. This was true before ARP, and continues to be the case today.

3. What are the NYSE's/SIAC's views on the soon-to-be re-released "Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System?"

The SEC has informed us that they will release the modified "Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" at the end of March 2003. Should the NYSE or our technology subsidiary, the Securities Industry Automation Corporation ("SIAC"), have comments on the revised paper once it is released, we will share them with you and the Subcommittee. I have attached the November 4, 2002 SIAC comment letter to the SEC which provided comments on the original white paper. I hope that it is helpful as part of the Subcommittee's review of business continuity planning.

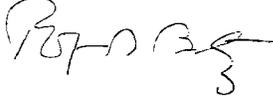
The NYSE wants to compliment the GAO for its professionalism in preparing their comprehensive report to examine the impact of the September 11 terrorist attacks on the financial markets. In many years of cooperation with GAO studies, we have found the GAO to be a fair, independent institution. This most recent review was no exception, and the GAO staff welcomed our comments and suggestions in preparing their report.

The NYSE is committed to ensuring that the U.S. capital markets remain the envy of the world and to insulating them from interruption by attack or natural catastrophe by protecting them from threats, by creating an infrastructure that can withstand attack or catastrophe, and by developing contingency plans that enable quick recovery.

In the event a terrorist attack or catastrophe achieves penetration and "takes out" our real-time redundant infrastructure, the NYSE is able to resume trading in a timely, fair and orderly fashion that will assure that every single one of America's \$5 million investors has access to our member firms and to us.

Mr. Chairman, I hope that the NYSE's thoughts and suggestions are helpful to you and the Subcommittee.

Sincerely yours,



Enclosure



Securities Industry Automation Corporation
Two MetroTech Center, Brooklyn, New York 11201

November 4, 2002

Jonathan G. Katz
Secretary
Securities and Exchange Commission
450 5th Street NW
Washington, DC 20549 -0609

SUBJECT: FILE NO 57-32-02 DRAFT INTERAGENCY WHITE PAPER ON SOUND PRACTICES TO STRENGTHEN THE RESILIENCE OF THE US FINANCIAL SYSTEM

Dear Mr. Katz:

Securities Industry Automation Corporation (SIAC) has, for the past 30 years, provided key system support to the New York and American Stock Exchanges, NSCC, DTCC, MBSCC, GSCC, EMCC and the securities industry nationwide. We, therefore, appreciate the opportunity to respond to the Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (the "White Paper").

The White Paper provides an important and thoughtful framework for the industry to examine its business continuity plans. We read the White Paper with a view towards assessing the reliability of the industry's systems and infrastructure, operational architectures and risk assumptions, when compared to the principles proposed in the White Paper.

Clearly, the business continuity issues facing the Financial Industry post 9/11 are significant and the strategy adopted by individual firms today will have a profound effect on the future of the industry. In our view, this strategy must address two fundamental questions. First, what are the risks, potential threats and probability of occurrence that we should protect against? Second, will the benefits of a given risk mitigation program justify the financial, operational and opportunity costs required for its implementation?

THREATS AND PROBABILITY OF OCCURRENCE

The White Paper preliminarily concludes that core clearing and settlement organizations and other firms that play significant roles in critical financial markets must develop risk mitigation plans which address a wide-scale regional disruption. We infer that by focusing on the wide-scale regional disruption, the agencies are assuming that local or "sub-regional" threats will be handled by some or all of the practices followed in the large scale case. The White Paper suggests that such a contingency plan must, as one of its baseline requirements, include the provision of an "out of region" backup or recovery

site, with technologies and architectures that will assure a 4 hour recovery and resumption of critical activities after an event.

This approach to the many types of threats could lead to a costly "one size fits all" mitigation strategy that may be less effective, difficult to implement and more costly than a more individually tailored program. We believe it is more appropriate for core organizations and firms to engage in a thorough analysis of individual threats and what each of those threats requires by way of mitigation. Some of these threats may have regional or national implications, but most will be localized. Any risk mitigation strategy should consider a number of factors including geographic location, the nature and effect of the potential threats, the probability of occurrence, the cost of remediation and the priority levels to be assigned to the restoration and resumption of certain functions and processes as may be appropriate.

Assuming that the dimensions and duration of an event will play a significant role in the development of mitigation strategies, the White Paper should address the following questions:

- What are the assumed threats that would cause a regional disruption and what are their assumed probabilities of occurrence?
- In the regional interruption scenario, what is the assumed duration? Is the region just inaccessible for some time period or have facilities, infrastructure and personnel received permanent damage?
- It is noteworthy that certain geographical regions have a higher probability of a regional disruption from natural threats than others. Should the guidelines address this issue?
- Does the single facility scenario assume a loss of the facility but the people assigned to it are available to move to another facility or is it the loss or unavailability of people assigned to that facility? What are the assumed duration, damage to facility and damage if any to personnel?

SERVICE LEVELS – RECOVERY AND RESUMPTION

We agree that common service level guidelines across the industry will help to ensure a resilient financial system which is highly interdependent on the core participants within the system. It is also crucial that service levels for processing be consistent with available technology and flexible enough to take advantage of new technologies.

We also believe that a wide-scale regional disruption, while imaginable, is of significantly lower probability than the vast number of business disruption scenarios of "sub-regional" impact. Further, intra-day recovery from a wide-scale regional disruption has special

- 3 -

requirements substantially above and beyond what is required for less catastrophic scenarios. We suggest that a goal of recovery from a wide-scale regional disruption in a matter of hours will not provide any "economies of scale" in dealing more effectively with the multitude of lesser disruption scenarios. Rather, the proposed guideline has the strong potential to significantly increase the overall cost and complexity of day-to-day operations management.

Moreover, the White Paper's reference to synchronous data transfers between redundant facilities implies a data recovery point objective of "time of failure." Is this service level required to mitigate a regional disruption or is there some acceptable data loss that could be tolerated? Currently, to achieve this synchronous level of transaction processing requires site separation distances of no more than approximately 60 miles.

GEOGRAPHICAL SEPARATION

We believe that the separation distance between redundant facilities should be determined by the threats that are being mitigated. While site separation is an important factor, it is one of several factors in the optimal solution.

The White Paper's concept of a "Region" is central to the question of how much distance between facilities is enough. A region is characterized by shared infrastructure providing critical services: telecommunications, power, and transportation. The event is assumed to cause a severe disruption of one or more of these services across the entire region, or to cause wide-scale evacuation or inaccessibility of the population within normal commuting range of the disruption's origin.

On September 11th, in addition to grievous loss of life, the business district of lower Manhattan lost significant telecommunications infrastructure. Power was disrupted in some areas. Transportation throughout New York City was severely curtailed and prioritized to support rescue missions and to forestall further attacks.

All clearance and settlement systems at SLAC - at both processing sites - were functional, and indeed were taken through their normal processing cycles without interruption. The most significant technical barrier to the resumption of business was the need to establish communications with firms' primary or contingency sites. All of this was accomplished within a few business days.

Our people, who live widely dispersed throughout the New York Metropolitan area, were able to reach our operating sites through different modes of transportation, and with help from government agencies overseeing the recovery. We were never short of staff to run our operations.

We suggest that large metropolitan areas, with a flexible array of infrastructure alternatives, and with governmental and core utility planning for contingencies have the

- 9 -

ability to respond effectively and rapidly to a major catastrophe. Put another way, the New York Metropolitan area was able to reconfigure itself to respond to this attack.

9/11 also demonstrated that distance does not address the multi-targeted attack, which is difficult to mitigate. The Pentagon is approximately 200 miles from the World Trade Center.

SOUND BUSINESS CONTINUITY PRACTICES

Hardening existing facilities within a region will reduce the probability of occurrence of single facility threats and, in addition, reduce the business impact of regional disruption threats. SLAC, as part of its normal operations prior to the events of September 11th, has taken steps to harden its infrastructure and continues to invest in this area to provide greater protection post 9/11.

For example, SLAC is implementing a Secure Financial Transaction Infrastructure (SFTI) network which is designed to mitigate the specific problems caused by the loss of data communications infrastructure in lower Manhattan. In the days following September 11th, SLAC's private internal networks and systems were completely functional, and this confirmed our long-held belief that auditable, diverse routes for critical telecommunications infrastructure are critically important for industry resilience.

Further extension of SFTI nationwide will provide an even greater diversified route structure for the industry. SFTI redundancy will be verifiable. Similar initiatives for other components of the infrastructure may improve the hardening of various regions.

CONCLUSION

We believe that the overwhelming majority of risks faced by the Industry - including risks similar to the 9/11 attack - can be, and in some cases have already been, substantially mitigated with straightforward extensions to existing business continuity practices.

We further believe that the relatively unique risk of the White Paper wide-scale regional disruption can be mitigated in a cost-effective way consistent with its likelihood, provided the time to recovery and resumption of services is appropriate given the catastrophic nature of such an event.

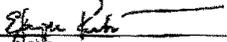
We believe that a "one size fits all" mitigation strategy will impose a significant cost and complexity burden on the Industry, in both financial and business process terms.

We believe that large metropolitan areas with robust and flexible telecommunications, power, and transportation infrastructures should be thought of as being made up of several "regions", and that reasonable business continuity assumptions can be made about the ability to work around a damaged "region" within that metropolitan area.

Finally, we believe mandating specific technical architectures or features for use in business continuity plans is inadvisable. Technology evolves rapidly, and our industry has historically shown a willingness to embrace and extend technologies to meet business needs.

We look forward to the continuation of this very important industry dialogue.

Sincerely,


E. Joseph Kibias
President and Co-Chief Operating Officer


Richard A. Edgar
President and Co-Chief Operating Officer