PROTECTING OUR FINANCIAL INFRASTRUCTURE: PREPARATION AND VIGILANCE

HEARING

BEFORE THE

COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

SEPTEMBER 8, 2004

Printed for the use of the Committee on Financial Services

Serial No. 108–108

U.S. GOVERNMENT PRINTING OFFICE

97–449 PDF WASHINGTON : 2004

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
RICHARD H. BAKER, Louisiana
SPENCER BACHUS, Alabama
MICHAEL N. CASTLE, Delaware
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
ROBERT W. NEY, Ohio
SUE W. KELLY, New York, *Vice Chair*
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
STEVEN C. LATOURETTE, Ohio
DONALD A. MANZULLO, Illinois
WALTER B. JONES, JR., North Carolina
DOUG OSE, California
JUDY BIGGERT, Illinois
MARK GREEN, Wisconsin
PATRICK J. TOOMEY, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN B. SHADEGG, Arizona
VITO FOSSELLA, New York
GARY G. MILLER, California
MELISSA A. HART, Pennsylvania
SHELLEY MOORE CAPITO, West Virginia
PATRICK J. TIBERI, Ohio
MARK R. KENNEDY, Minnesota
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
TIM MURPHY, Pennsylvania
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
KATHERINE HARRIS, Florida
RICK RENZI, Arizona

BARNEY FRANK, Massachusetts
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELÁZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
BARBARA LEE, California
JAY INSLEE, Washington
DENNIS MOORE, Kansas
MICHAEL E. CAPUANO, Massachusetts
HAROLD E. FORD, JR., Tennessee
RUBÉN HINOJOSA, Texas
KEN LUCAS, Kentucky
JOSEPH CROWLEY, New York
WM. LACY CLAY, Missouri
STEVE ISRAEL, New York
MIKE ROSS, Arkansas
CAROLYN MCCARTHY, New York
JOE BACA, California
JIM MATHESON, Utah
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
RAHM EMANUEL, Illinois
DAVID SCOTT, Georgia
ARTUR DAVIS, Alabama
CHRIS BELL, Texas

BERNARD SANDERS, Vermont

ROBERT U. FOSTER, III, *Staff Director*

CONTENTS

	Page
Hearing held on:	
September 8, 2004	1
Appendix:	
September 8, 2004	47

WITNESSES

WEDNESDAY, SEPTEMBER 8, 2004

Abernathy, Hon. Wayne, Assistant Secretary for Financial Institutions, Department of Treasury	10
Britz, Robert G., President and Co-Chief Operating Officer, New York Stock Exchange, Inc.	29
Dolloff, Wilton, Executive Vice President, Operations and Technology, Huntington Bancshares Incorporated, on behalf of Bits and The Financial Services Roundtable	34
Gaer, Samuel, Chief Information Officer, NY Mercantile Exchange	36
Liscouski, Robert, Assistant Secretary, Information Analysis and Infrastructure Protection, Department of Homeland Security	11
Mohr, John, Executive Vice President, The Clearing House Association L.L.C	32
Olson, Hon. Mark W., Member, Board of Governors, Federal Reserve System	8
Tishuk, Brian S., Executive Director, ChicagoFIRST	38

APPENDIX

Prepared statements:	
Oxley, Hon. Michael G.	48
Bachus, Hon. Spencer	50
Emanuel, Hon. Rahm	52
Gillmor, Hon. Paul E.	53
Hinojosa, Hon. Rubén	55
Kelly, Hon. Sue W.	57
Abernathy, Hon. Wayne	59
Britz, Robert G.	65
Dolloff, Wilton	86
Gaer, Samuel	101
Liscouski, Robert	109
Mohr, John	116
Olson, Hon. Mark W.	125
Tishuk, Brian S.	136

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Britz, Robert G.:	
Written response to questions from Hon. Rubén Hinojosa	151
Olson, Hon. Mark W.:	
Written response to questions from Hon. Spencer Bachus	152
Written response to questions from Hon. Rubén Hinojosa	155
Tishuk, Brian S.:	
Written response to questions from Hon. Rubén Hinojosa	158

PROTECTING OUR FINANCIAL INFRASTRUCTURE: PREPARATION AND VIGILANCE

Wednesday, September 8, 2004

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The committee met, pursuant to call, at 10:07 a.m., in Room 2128, Rayburn House Office Building, Hon. Michael Oxley [chairman of the committee] presiding.

Present: Representatives Leach, Bachus, Kelly, Biggert, Miller of California, Capito, Tiberi, Brown-Waite, Frank, Maloney, Gutierrez, Ackerman, Sherman, Lee, Inslee, Hinojosa, Lucas of Kentucky, Matheson, Miller of North Carolina, Emanuel, Scott, and Bell.

Mrs. KELLY. [Presiding.] This hearing of the committee will come to order.

This morning the committee convenes to continue its ongoing oversight of preparedness incident recovery and critical infrastructure protection issues. I thank Chairman Oxley for holding this hearing.

At the heart of critical infrastructure is the safety and soundness of the financial services sector which drives every aspect of our economy. Earlier this Congress, the Oversight and Investigations Subcommittee held a hearing to examine the state of readiness of the financial services sector and the critical infrastructure that allows it to serve our country. In that hearing, the subcommittee learned about many promising steps that have been taken by our financial caretakers, as well as the constant assessment and improvements that still must be performed.

Over the last several years, our country has experienced many extraordinary events that have threatened the safety of the American people and of our financial system, from the horrific attacks of September 11, 2001 to the blackouts and hurricanes, but fortunately our markets have experienced remarkably quick recoveries, illustrating the tremendous resiliency of the financial system and the U.S. economy.

As a result of these events, it is apparent that the technology age we live in, which allows us to provide services and access information in a heartbeat, is both a boon and one of our greatest vulnerabilities. It is imperative that we continually revise our efforts to protect data systems and the infrastructure that allow them to operate, which are ever more entwined and dependent on one another.

Today, this review could not be any more timely. Last month, Department of Homeland Security Secretary Tom Ridge issued a warning of possible al Qaeda terrorist attacks to our financial institutions, including the Prudential Financial, the Citigroup Center Building, and the New York Stock Exchange, as well as the International Monetary Fund and World Bank buildings. The committee is very interested in the steps that have been taken to protect our financial infrastructure since the threat level was elevated to code orange for the financial services sector in New York City, Northern New Jersey and here in Washington, D.C.

As terrorists continue to target our economy and financial institutions, we must ensure our financial infrastructure is strong enough to withstand diverse types of attacks. We must ensure that all our systems, whether financial, energy, transportation or telecommunications, are able to operate under extraordinary circumstances.

The committee is pleased to have with us this morning Federal Reserve Board Chairman Mark Olson, who has been a leader in these efforts in his role at the Fed. We also welcome the Assistant Secretary for Financial Institutions at the Treasury Department, Wayne Abernathy, who also serves as the department's sector coordinator for critical infrastructure protection. And joining us is the Assistant Secretary of Homeland Security for Infrastructure Robert Liscouski, who is responsible for the department's efforts to identify our critical infrastructures and propose protective measures to keep them safe from terrorist attacks.

Keeping our financial systems functioning and safe requires a high degree of coordination between many different and important parties, both public and private. The committee is also pleased to have with us witnesses on our second panel who are leaders in protecting critical financial services assets from major disasters, including several individuals from the great State of New York. These witnesses, along with others in the private sector and the government who could not be represented here today, are working in the field every day to protect our financial systems.

The committee thanks all of our witnesses today for your appearance, and we look forward to your testimony. Together, we hope that we can ensure that our financial systems are functioning smoothly under all circumstances and the American people should have full confidence in the financial services sector.

[The prepared statement of Hon. Sue W. Kelly can be found on page 57 in the appendix.]

Mrs. KELLY. I would like to now recognize my colleague, Ms. Maloney.

Mrs. MALONEY. Thank you very much. I join you in thanking Chairman Oxley and Ranking Member Frank and my colleague from the great State of New York for chairing this meeting. I welcome all of our witnesses, who include a number of organizations that I am privileged to represent. Some of them are my constituents.

In New York City, the heart of the nation's financial infrastructure, we can vividly remember what it was like to have that infrastructure damaged by terrorist attack just 3 years ago. We know very well the extraordinary lengths that many of New York's fine

institutions, some of which are represented here today, went to ensure that the financial markets functioned as soon as possible to protect not only the U.S. economy, but that of the world from irreversible harm. I do not think any of us will forget the anticipation, the anxiety before the big boards opened up again and were there to serve the people. These terrible events demonstrated clearly that the protection of our financial infrastructure is essential to the nation's financial system. Unfortunately, they also demonstrated that we were ill-prepared for an attack on it.

So my fundamental question today, to each of the private sector witnesses represented today, is what would happen differently today. My even more basic question to Treasury, the Fed and Homeland Security is who would be in charge of the government response. I would like to hear that there is an established, tested and proven system of coordination and a clear line of authority and accountability so that decisions can be made in a prompt and informed manner, but I am not sure that that is the case.

We have several new committees, the Financial and Banking Information Infrastructure Committee, the Financial Service Sector Coordinating Council, and the Financial Services Information-Sharing and Analysis Center. But how exactly do they work in practice? Who makes the final call? Who staffs these committees? And who is responsible for carrying out their decisions?

I would like to hear how our response system held up last month when the terror level was raised for financial institutions in New York City and elsewhere. I would also like to hear how that system is working now to ensure a speedy and sufficient response to the danger posed by Hurricane Frances to the financial institutions in its path. We, this committee, know the government is capable of a sustained and coherent response to threats to the financial infrastructure.

As those of us who have served on this committee know, we were prepared for the Y2K threat. There were many hearings, the government response, and many oversight hearings. But as the 9/11 Commission reports, that effort relaxed after the millennium passed and the government was not well coordinated nor was key information properly shared among various agencies or with the private sector in the months leading up to September 11.

One year after September 11, this committee asked the General Accounting Office to report on what additional steps had been taken to protect the financial infrastructure since that catastrophe. The GAO report, which was the last government report issued on this subject in February of 2003, gave regulators and firms a mixed assessment, criticizing them for having focused on clearing and settlement activity, to the exclusion of trading and retail firms.

Our Oversight Committee reviewed the ground again in October of 2003 in the context of the August 2003 blackout, and we had the pleasure of hearing from many of our panelists today. As a New Yorker, I am proud of the way in which the public and private financial sectors of my city worked together to respond to these two tremendous disasters and are continuing to work with the federal government.

Such efforts demonstrate that our cities are prepared to protect their financial industry and that the calls some have made for fi-

nancial institutions to create backup locations hundreds of miles away from an urban area are totally misguided. They can have them in a different area of the urban area. Congress and the federal government should support the hubs of our nation's finance by providing additional homeland security funding to them and by assisting them in identifying and protecting the critical elements of our financial infrastructure that they possess.

So as we sit here today, we have recent reminders of how crucial it is constantly to review and refine the safeguards of our financial infrastructure. I look forward to hearing from our witnesses what they have done to protect the physical body of the nation's financial system from harm, and what we can do to be of assistance in that effort.

I thank all the panelists for being here and yield back my balance.

Mrs. KELLY. Thank you very much.

Mr. Bachus?

Mr. BACHUS. I thank the Chairman.

I would say in response to what Ms. Maloney said, that of course the structure for responding to a terrorist attack actually was established back in 1998 by Presidential Decision Directive 63, signed by President Clinton. Then it was refined by Executive Order by President Bush right after 9/11. I think that the experience that we had on 9/11, that experience was that our financial markets are very resilient and that we were in fact prepared for something which is almost impossible to be prepared for, something we never faced before. But the financial markets functioned very well, and showed a great amount of resilience.

Despite the infrastructure damage to the World Trade towers and actually the physical loss of the facilities, the market operations recovered very quickly. I think we are all amazed at how quickly they responded. I think that is very good news. The GAO did make certain recommendations, but again a lot of what you all focused on was because really you were directed to focus on those things. I think all in all, clearing and settlement, if you do not focus on those things, you have a real problem. As far as retail firms and trading organizations, I think since the last year and a half, and we are going to hear from our second panel, you have done a great deal to focus on that. I know the latest threat is what the two speakers before are focused on, was actually car bombs or a bomb which would take out some physical structure.

But you are actually, our first panel, you are the designated people under the presidential directives to be in charge, and the designated agency for our financial institutions is the Treasury Department, working with other organizations. So I think the underlying message ought to be that financial institutions, our financial markets performed very well under a tremendous attack. The market did not recover, but that was a result of just market factors and facing a new threat, and the facts of uncertainty in the world, not anything to do actually with the inability of the markets to operate.

I would also say, and I am sure that there will be a question addressing this, there are certain things that you have asked us to do, and one of them is the netting provisions, which in the Congress, we passed it out of the House, but the Senate has never

taken it up. You have identified that as one of your top priorities in case of another financial attack. So this Congress really has failed to do some of the things that you have said are most important.

So with that, I end my comments, but I applaud the administration for everything they have done.

[The prepared statement of Hon. Spencer Bachus can be found on page 50 in the appendix.]

Mrs. KELLY. Thank you very much.

Mr. Hinojosa?

Mr. HINOJOSA. Thank you, Chairwoman Kelly.

I want to thank you and Ranking Member Frank for holding this very important hearing today.

The United States needs to remain prepared for any and all terrorist attacks following the horror that we endured on 9/11. We need to remain vigilant to ensure that similar attacks never happen again on U.S. soil.

As I noted during the committee's hearing on the 9/11 Commission report during the August recess, we here in the United States need to focus on increasing the security of our own documentation such as driver's licenses, passports, and visas in order to prevent such terrorists from entering the United States again. The 9/11 Commission Vice Chairman Lee Hamilton agreed that we need to increase the security of our own documentation and such measures should include requiring biometric information and security features such as fingerprints, digitized photos, holograms and serial numbers on these types of documents, and increasing the technology with which financial institutions can verify IDs.

Prior to 9/11, the United States consulate that required biometric information from individuals seeking entry into the United States was the U.S. consulate in Mexico. Such biometric data and more is now included as part of the 12 security features Mexico added to the matricula consular ID card in 2002. As the Washington Times noted some time ago, the updated matricula consular ID card is more secure than many of our U.S. documents. Perhaps we should emulate the security features incorporated into the card as we create a new, more secure system of documentation in the United States.

The U.S. was very lucky that the 9/11 terrorist attacks did not completely halt the free flow of the U.S. capital markets for very long. Granted, the New York Stock Exchange and others closed down for a short time, and certain Federal Reserve Bank airplanes were unable to fly for a time due to the flight restrictions following the terrorist attacks. These Federal Reserve flights are an integral part of the payment clearinghouse system in the United States. Nonetheless, I was very impressed by the ability of the New York Stock Exchange to adapt quickly to the terrorist situation and to accommodate the trades of so many exchanges on its own system in the days following 9/11.

I ask that the balance of my opening statement be included, Madam Chair.

[The prepared statement of Hon. Rubén Hinojosa can be found on page 55 in the appendix.]

Mrs. KELLY. Of course. We would be glad to include the opening statement of anyone of the members of this committee, and it is so moved.

Mr. Leach, have you an opening statement?

Mr. LEACH. Just briefly. Just very briefly let me mention a couple of things by perspective. As everybody in banking knows, a century ago a famous bank robber once commented that, why do you rob banks? You do it because that is where the money is. But the interesting aspect about the modern financial system is that financial institutions and trading institutions are not where the money is. It is simply where assets are traded and kept track of. Great violence applied to a bank; great violence applied to a trading institution in one sense does not destroy a lot of assets. It destroys to some degree or disrupts tracking mechanisms, but if there is good redundancy, the system itself can be not harmed gravely. So redundancy is really the issue.

Secondly, I think that we ought to beware that even though it is true that Congress has really been slacking in its discipline in not putting forth a netting bill, which is a very important bill and one which I have long advocated, and it is not done largely because we have problems that related to inter-institutional committees of jurisdiction, but hopefully it will happen this year. But the big issue is, what happens if there is a calamity? Here, the great aspect of perspective is that we have had for many decades authorized an institution of the United States Government, the Federal Reserve, to liquefy any calamity anywhere in the world, but particularly in the United States. So if something awful were to happen to a financial institution, the Fed is there to make sure the system can be sustaining.

I only say this because acts against the financial community are acts of barbarism, but they are not acts that bring down the American system. They are simply acts of barbarism. Everybody in the private and public sector has to be very concerned that we get any system that goes down, up and running again, but that can happen. The American system will not be affected as a country. It will simply be a disruption. That is the way we have to work at it because we cannot perfectly protect anybody and anything.

Let me just in conclusion say, because I tried to discount the importance of the netting bill, let me raise its importance again. It is really irresponsible that Congress has not acted yet to put forth a bill that settles derivatives-type trading instruments on an orderly basis instantaneously. We are obligated to do that and I am hopeful that that will happen this fall.

Thank you, Madam Chairman.

Mrs. KELLY. We turn now to Mr. Gutierrez.

Mr. GUTIERREZ. Good morning and thank you, Madam Chairman, for calling this hearing on protecting our nation's financial infrastructure. I am particularly pleased that we will be hearing from Brian Tishuk of ChicagoFIRST, an organization composed of Chicago's primary financial institutions that was formed to address these various issues.

ChicagoFIRST is an excellent example of a public-private partnership that should serve as a model for other regions. We will be hearing in detail about the formation of the organization, which

was not an easy task. We will also hear about their recent tabletop exercise which tested the partnership's ability to function under the threat of a terrorist attack. At the appropriate time, I will be asking the Department of Homeland Security about certain matters in the written testimony, specifically the fact that ChicagoFIRST has discussed with DHS its interest in hardening Chicago in general and the financial district specifically.

As part of that, ChicagoFIRST has recommended funding for certain equipment being sought by both the City of Chicago and ChicagoFIRST; the placement of a DHS center in Chicago; and has asked for DHS's help in procuring security clearances for certain financial representatives so that they can participate more actively in the protection of the city's financial infrastructure. These recommendations and requests have apparently gone unheeded and no answers have been forthcoming from Homeland Security to ChicagoFIRST. I will be asking DHS, though it has been helpful to ChicagoFIRST, if it could take more of an initiative to reaching out to financial centers other than Chicago to promote regional partnerships.

I wish to thank my colleague, Congressman Emanuel, for his request that ChicagoFIRST testify before us, and I look forward to the testimony, as well as the testimony of the other witnesses.

Thank you, Madam Chairman.

Mrs. KELLY. Thank you very much, Mr. Gutierrez.

Mr. Scott.

Mr. SCOTT. Thank you very much, Chairlady.

This is a very timely hearing, and I, like many people across this nation, am quite worried about another possible attack. I certainly want to thank Chairman Oxley and Ranking Member Frank, Ms. Kelly, for holding these hearings today.

The recent warnings of attacks on financial services targets caused no disruption to financial activity. However, concrete Jersey barriers have multiplied around New York and Washington. While these temporary barriers provide some cosmetic protections against potential terrorist attacks such as car bombs, what about suicide bombers who could very well just be walking Wall Street or any of the streets in the area or any of the streets in Washington, D.C., and get very close to us, as we have seen from other places around the world?

To be prepared, to be vigilant, we need to know concretely, what is the role of our Federal Reserve? What is the role of our Treasury Department? How are their roles coordinated with our basic intelligence agencies of the CIA, the FBI and the Defense and State Departments's intelligence agencies, of what is happening around the world in other financial capitals? I would be very interested to hear your response in terms of our reshuffling the deck on our intelligence operations to see if our financial services industry's intelligence apparatus will work better under a new general authority of an intelligence czar.

I think further also we have to work to prevent attacks by monitoring and by detecting terrorists. Let us take a look at certain organized crime groups that work concretely with terrorist organizations. I think also that we are going to have to look at other areas, our computer systems, our telecommunications networks, our elec-

trical power grids, our transportation systems, how all of those work. Also, terrorist organizations may be targeting cities other than New York and Washington, D.C. And maybe they may be even more likely targets, regional financial centers like Atlanta, Chicago, San Francisco, and Houston.

It is important that the financial infrastructure include regional plans to address these threats. For example, federal agents recently arrested a man from Pakistan who was videotaping buildings in several southern cities, including my own city of Atlanta. And other regional threats, that would be power failures, natural disasters.

Certainly, as Congress reviews the financial services industry's readiness to respond to attacks, we must also work to ensure that any attacks do not cause long-term damage on creditworthiness of innocent consumers. And then finally looking at the world, and the impact of how, for example, a terrorist attack on a financial center such as Tokyo or Paris would have on our financial system, this particularly in view of the fact that we are the world's leading financial center.

These and many other questions I look forward to examining. I think this is a very important hearing this morning, and I look forward to each of your testimonies.

Thank you, Madam Chair.

Mrs. KELLY. Thank you, Mr. Scott.

Without objection, all members' opening statements will be made part of the record.

We turn now to our first panel. We have three witnesses on our first panel: The Honorable Mark W. Olson, member of the Board of Governors, Federal Reserve. We have the Honorable Wayne Abernathy, Assistant Secretary of the Treasury for Financial Institutions, Department of Treasury. And we have the Honorable Robert Liscouski, Assistant Secretary of Homeland Security for Infrastructure Protection.

Without objection, your written statements will be made part of the record. You will each be recognized for a 5-minute summary of your testimony. I am sure that all of you have testified in front of these committees before, so I do not need to explain the lighting system.

Mr. Olson, let us begin with you.

STATEMENT OF HON. MARK W. OLSON, MEMBER, BOARD OF GOVERNORS, FEDERAL RESERVE SYSTEM

Mr. OLSON. Thank you very much, Chairwoman Kelly. We thank you, Ranking Member Frank, Chairman Oxley and members of the committee for holding this hearing. I agree with all of the members who have acknowledged that this is an important subject and a very timely subject.

A number of questions have come up. I would be happy to address them as the questioning goes around, but let me just open by talking about three specific points that I would like to highlight. First, many of you started your opening remarks by talking about the efforts of 9/11. Of course, that was what constituted the start of a new era for us in terms of our recognition of both the exposure

to terrorism activities and other threats to the financial services system.

The Federal Reserve, of course, responded that day by providing, among other things, $100 billion of liquidity into the financial services system, as Congressman Leach alluded to in his opening remarks. I think that the resilience of the system at that point was demonstrated by a number of facts. Number one, the fact that the Fed over the course of a 5-day, in fact even a several-week period, responded in a different way providing either liquidity or overdraft protection or responding to changing needs as a result of the excesses of float that were building up in some parts of the system.

We also initiated the swap lines for currencies with other central banks, indicating the cooperation internationally that we have been able to achieve and had achieved up to that point. Beyond that point, the Fed then began to look at its own resiliency. We initiated 40 different efforts to test our own ability to provide financial services, the redundancy necessary to provide the financial services, and the ability to sustain operations over a period of time.

I would point out that on 9/11, the Federal Reserve Bank of New York did not close; that last weekend with the hurricane in Miami, the Miami Fed and Jacksonville Fed did not close. So we have a very strong track record of being able to meet those needs.

Beyond our own efforts, of course, an interagency team produced a white paper involving the Fed, the Comptroller of the Currency, and the SEC, where we identified the requirements of the critical financial institutions in order to meet clearing and settlement responsibilities on an ongoing basis, and in order to meet the critical functions of the financial services network. For each of the institutions that have been identified, a target deadline has been set to achieve the level of readiness which is anticipated either in 2005 or 2006, depending on their starting points.

Additionally, and this is the point that a number of you alluded to, there is a heightened level of cooperation among the federal agencies and within the private sector. The Treasury Department has been designated as the lead as sector liaison, and we have been happy to work with them. I think the resilience of it and the importance of it was brought out in response to the elevation to code orange under the direction of Homeland Security. In our judgment, that worked very well and we achieved a state of readiness very rapidly after the information was made available.

Indeed, Congresswoman and members of the committee, we feel that the financial institutions sector has progressed in a very significant way over the course of the past several years, particularly the last 3 years, and it continues to improve. It is a moving target, as we learn more about the potential threat. As Congressman Scott suggested, we need to adjust as new information is produced, and we have done so.

I would be happy to answer questions when my time comes.

[The prepared statement of Hon. Mark W. Olson can be found on page 125 in the appendix.]

Mrs. KELLY. Thank you very much, Mr. Olson.

Mr. Abernathy.

STATEMENT OF HON. WAYNE ABERNATHY, ASSISTANT SECRETARY FOR FINANCIAL INSTITUTIONS, U.S. DEPARTMENT OF TREASURY

Mr. ABERNATHY. Chairwoman Kelly, Ranking Member Frank, members of the committee, I am pleased to tell you that the financial services sector is in a state of advanced readiness and preparation, and that it handled well the recent information about terrorist targeting of specific institutions. Customers were able to continue business as usual. While there was concern, there was no crisis. There was no panic, but rather activation of planned steps to mitigate exposure to risks. I applaud our intelligence and law enforcement agencies for obtaining this vital information and promptly sharing it with the affected institutions.

President Bush has led the development and implementation of an effective program to defend our country against terrorism. Protection of our financial infrastructure is a key element of that program and much valuable work has already been done. That is because we have long known in general what recent information has reaffirmed with specificity, that our financial institutions are being targeted by our enemies. They are under assault every day. Most of these assaults are in the nature of electronic or cyber attacks such as computer viruses, trojans, worms and various forms of financial fraud, including fishing and spoofing. These assaults have progressed from computer hackers and pranksters into theft, and now we believe on to schemes to disrupt organizations and operations.

Some of these attacks have their sources in organized crime. Increasingly, still more sinister actors are involved. I do not say this to be alarmist, but rather to make the point that our financial institutions have for some time now been operating in a dangerous environment, and they are becoming increasingly adept at doing so successfully. This success is a result of careful organization and hard work by the private sector and government agencies at all levels.

The organized government effort today is based upon a directive from President Bush, Homeland Security Presidential Directive 7. This is a flexible, coordinated program that works well in marshaling resources and activities. HSPD-7 places upon the Department of Homeland Security the central responsibility for coordinating the overall national program. The directive relies upon specific agencies to take the immediate lead, ensuring that critical protection efforts will be led by departments that have the expertise and experience. Treasury is the lead agency for the banking and finance sector.

Nearly all of the financial infrastructure is owned by the private sector. We work closely with the private sector through reliance upon several organizations. Chief among these is the Financial Services Sector Coordinating Council or FSSCC, the chairman of which is appointed by the Treasury secretary. The current chairman is Don Donahue, a senior officer of the Depository Trust & Clearing Corporation in New York City. The FSSCC is made up of entities and trade associations representing virtually every financial institution in the nation.

Alongside the FSSCC is the Financial Services Information-Sharing and Analysis Center, or FS-ISAC, the chief communications system for the sector on a wide variety of threats and challenges. Last year, Treasury devoted $2 million to develop and implement a plan for broadening the reach of the FS-ISAC. In the last couple of weeks, Federal Housing Finance Board Chairman Alicia Castaneda and I sent a joint letter to each of the federal home loan banks encouraging them to join the FS-ISAC. We continue to encourage all financial institutions to sign up.

Under the sponsorship of the President's Working Group on Financial Markets, and chaired by the Treasury, the Financial and Banking Information Infrastructure Committee, or FBIIC, brings together representatives of all of the federal and state financial regulators. A cardinal rule of the FBIIC and the key to its success and achievement over the last several years is the principle of responsibility. The FBIIC does not try to take over the responsibility or interfere in the work of any agency. What the FBIIC provides is a means of coordinating efforts, sharing best practices, pooling talents and resources, facilitating communication, encouraging wherever possible and cajoling where necessary.

While terrorist threats themselves are bad news, I see much good news in our latest experience. Our antiterrorism efforts are bearing fruit, providing valuable information that is being applied and acted upon appropriately by the financial sector just as soon as it is made available, without disruption or degradation of services. The success of the collective actions of the federal, state and local governments and the preparedness and response of the private sector are progressively denying terrorists their objective, their goal of disrupting our free markets. Freedom and free markets are the targets of the terrorists, and we are showing that we can harness the power of free people and free institutions to defeat the terrorists.

So in conclusion, there is much work yet to do, but tremendous work has already been done. Our markets are deeper, more resilient than ever before, and they are becoming more so every day.

Thank you.

[The prepared statement of Hon. Wayne Abernathy can be found on page 59 in the appendix.]

Mrs. KELLY. Thank you, Mr. Abernathy.

Mr. Liscouski.

STATEMENT OF ROBERT LISCOUSKI, ASSISTANT SECRETARY, INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY

Mr. LISCOUSKI. Good morning and thank you, Chairwoman Kelly and Ranking Member Frank and distinguished members of the committee. It is a pleasure to be before you this morning to discuss the protections that we have with the financial services sector. I am going to address some of the comments specifically in the question-answer period, but I would like to give an overview of where we are today in working with the Department of Treasury and the Fed.

The Office of Infrastructure Protection specifically has focused on monitoring and assessing threats and vulnerabilities to all sectors, including the banking and the financial services sector. Before I

begin, I would like to recognize the efforts of the Department of Treasury and the Fed, and commend them for their leadership to organize and take the first steps to protect the financial infrastructure prior to September 11.

Subsequent to the creation of the Department of Homeland Security, the Treasury Department and the Fed have been key partners with DHS in continuing the execution of our efforts to protect our critical infrastructure. In preparation for responding to threats and elevated threat levels, my office and the directorate for which I work, IAIP, has been building and coordinating a two-way exchange of information with the public and private sectors. These efforts have also included building relationships with the private sector and government entities, as well as implementing and integrating technical and information-sharing solutions.

The financial services sector has developed two effective mechanisms for two-way information sharing. The Financial Services Sector Coordinating Council, the FSSCC, as Assistant Secretary Abernathy just described, consists of senior representatives of major financial institutions representing a cross-section of the financial industry. The second component, the Financial Services Information Sharing and Analysis Center, the FS-ISAC, provides a mechanism for gathering and analyzing and appropriately sanitizing and subsequently disseminating information to and from its members and the federal government. The FS-ISAC conducts threat intelligence conference calls periodically at the unclassified level for subscriber members. With IAIP providing input, these calls cover physical and cyber-threats and vulnerabilities and incidents that have recently occurred. It includes suggestions and recommended proactive actions that can be taken to mitigate the threats.

Sector coordinating councils and their ISACs maintain and provide DHS with distribution lists, which allow them to quickly disseminate threat warnings, alerts and advisories to members of their sectors. Information provided by the sectors is incorporated into the situational awareness picture, together along with the intelligence community's information and the law enforcement community concerning possible threats to the nation's critical infrastructures.

The sectors are also capable of initiating crisis conference calls within an hour of notification via a crisis alert. In addition, DHS has established close working relationships with the appropriately cleared senior sector members such as the financial services sector to provide classified information relevant to the threat environment.

The interconnected and interdependent nature of our infrastructure makes our physical and cyber-assets difficult to separate and therefore it would be ineffective and inefficient to address them in isolation. Consequently, my office integrates both the strategy and the tactics necessary for the appropriate protection of the cyber, physical and people assets in concert. In working with the infrastructure protection office of the United States secret service, for example, it recently joined forces with the Carnegie-Mellon University Software Engineering Institute's CERT Coordination Center, CERT/CC, in order to conduct an analysis of the insider threat.

The insider threat study is a collaborative effort to better understand the insider activities affecting information systems and data in critical infrastructure sectors, to include the banking and finance sector. The insider threat study examined incidents involving employees who intentionally exceeded or misused an authorized level of system access that affected the organization's data, daily business operations, systems security, or other areas via computer. The study focused on online behaviors and communications in which the insiders engaged prior to the incidents.

On August 24 of this year, the first part of the report was released to the public sector. It is referenced as the Insider Threat Study Elicits Cyber-Activity in the Banking and Finance Sector. This portion of the report focused on individuals who have had the access and perpetrated harm using information systems in the banking and finance sector, which includes credit unions, banks, investment firms, credit bureaus, and the financial institutions. The findings highlighted in this area of the report are of great benefit to the financial sector and provided concrete examples of how insiders accomplish their activities and offered suggestions on what security and policy procedures might deter or prevent future activity.

I would like to discuss now the latest series of threats against U.S. financial institutions spurred by ongoing concerns over al Qaeda's interest in targeting U.S. critical infrastructure, as well as recent intelligence revelations of detailed reconnaissance of several U.S. financial institutions. The level and specificity of information found was alarming, prompting DHS to recommend raising the threat level of orange for the financial services sector in New York, Northern New Jersey and Washington, D.C. on August 1. This was the first time the level had been changed for an individual sector and geographic-specific location.

In response to the heightened threat level, IAIP acted on several fronts in coordination with Treasury and Fed to address the threat. Conference calls were arranged between DHS, industry leaders, chief security officers, state and homeland security officials, and local law enforcement officials, and with numerous financial institutions. Our relationship and communications with the private sector security leadership for the affected institutions particularly were key to our overall approach on how to effectively manage the threat situation.

We provided immediate alerts to the financial sector regarding the threat and we continued to work with the industry to ensure that all targeted financial institutions were individually briefed. IAIP coordinated with federal, state and local law enforcement entities to ensure that the appropriate information was exchanged between government and the private sector.

We also polled the various financial institutions to determine what additional protective measures were needed for implementation as a result of the heightened alert period. We dispatched personnel immediately to the facilities in Washington, New York and Northern New Jersey to conduct site-assist visits, which would evaluate the recommended security measures in collaboration with local law enforcement officials and asset-owners and operators to

ensure that the appropriate vulnerabilities were identified and remediation measures were taken.

In addition to the site-assist visits, IAIP personnel have been working with the individual facilities and local law enforcement to create buffer zones around the most critical facilities. These are community-based efforts focused on rapidly reducing vulnerabilities outside the fence of an institution or facility to select critical infrastructure components in key resources. We work closely with the law enforcement community and the private sector to ensure that these plans and implementation strategies are effective and efficient.

As I have discussed with you today, IAIP has taken many actions to secure the financial services sector, in partnership with treasury and the Fed, and we have laid a foundation for a true partnership with the public and private sector. Based on this foundation, with continued dedication we will continue to work to protect the nation's critical infrastructure.

Thank you for the opportunity today and look forward to your questions.

[The prepared statement of Robert Liscouski can be found on page 109 in the appendix.]

Mrs. KELLY. Thank you very much, Mr. Liscouski.

I would like to ask you about a question you just brought up. Mr. Liscouski, you mentioned the Carnegie study, and you talked about the insider threat. My first question, does it make any difference? You talked earlier about the department working with financial institutions and software companies to identify vulnerabilities and to design enhanced software assurance practices. Does it make any difference if these vulnerabilities are international or if they are home-grown?

Mr. LISCOUSKI. The concern you raise is a valid one, particularly because of the way software is deployed throughout our critical infrastructure at-large and particularly in the banking and finance sector. Let me just preface my remarks by saying a holistic security program has to consider all elements of security. So it is a physical security approach, cyber as well as personnel security. The software assurance practices that you are discussing also include insurance that software is developed and engineered to the appropriate specs and standards and there are quality assurance conducted on software before it is shipped out.

So when we talk about internationally developed software or that which is outsourced internationally versus that which is developed here in the United States, the first point in securing an institution, whether it be a banking institution or other critical infrastructure component, is to ensure that the appropriate procedures and mechanisms, the people and process part of the security approach, is taken.

We cannot take a slice of that pie and examine it independently for its vulnerabilities without examining the interdependencies of the entire process. So we alleviate those concerns by assuring that best practices are followed within institutions, within critical infrastructure components, and good policies and procedures and security practices are set up, so we can mitigate the potential effects of any software vulnerability, irrespective of whether it is inter-

nationally developed or developed by an international company abroad or domestically.

So the insider threat study looks at ways that those exploits could be manifested or can be exploited, and it looks at ways that security procedures and processes can be put in place to help mitigate that risk.

Mrs. KELLY. What recommendations did the study make? Have you additional recommendations? Would you care to share that with the committee?

Mr. LISCOUSKI. Yes, ma'am. I would refer to the report specifically. I apologize for not having a copy in front of me, but my recollection of the report, and I can validate this in writing to you later, it did not specifically address software development in the context of insider threat. It looked more from the perspective of the insider threat as a trusted user on a system, and therefore someone who potentially could abuse their trusted access internally to an organization.

So in the context of that part of the study, there were a variety of recommendations made for procedures and policies which would limit a person's access, but yet balancing the need for conducting business. So it focused on behavioral aspects of insiders that might foretell that there was a problem, as well as recommended policies that could help mitigate those threats.

Mrs. KELLY. Thank you. I want to ask one other question of you, sir. What sorts of warning signs should financial institutions be looking for in the case of both physical and cyber attacks? Are there warning signs out there that these institutions should be looking for?

Mr. LISCOUSKI. Yes, ma'am. I think this past month, in August and the end of July when we received the threat information is a good indicator or a good example of how those warning signs can be manifested. What we learned from the casing reports that were exploited from the information we received that resulted in the threat warning going up was that there is oftentimes detailed surveillance occurring at financial institutions and other critical infrastructure components which are observable behaviors. And subsequently, as we have indicated, these precursors or pre-incident indicators of terrorist activity resulting in surveillance, anomalous types of activities that can be observed need to be communicated.

So what the lesson from that was that that information was shared with the private sector, the banking institutions in this case and the financial institutions, to be shared with their security personnel, and those folks were in a position to observe anomalous behavior and report that back. So the types of attacks that we are concerned about in this particular case were typically kinetic or bombing types of attacks, those which would require a breach of a perimeter and some sort of pre-operational surveillance to identify the vulnerabilities of a particular institution. Those things are all observable, and if they are observed and reported, we can get an indication of what is occurring pre-incident, just as an example of something that was shared.

Mrs. KELLY. You looked at bombing attacks, did you say, but you have also looked at the cyber-threats. So you have looked at both sides of what is happening.

Mr. LISCOUSKI. That is correct. In the context of the recent threat, the job of my office is precisely looking at the nexus of all threats, irrespective of if they seem to be dominated by a physical threat as in this case initially. We take a very detailed look at the cyber-environment to see if there is any activity that would indicate that a specific institution is being targeted as a result of various types of probing. So we consider all the threats, either cyber or physical or the people aspect of it, in concert when we get threat information.

In this particular case, we had no evidence that there was a cyber-threat manifesting itself in the context of this particular physical threat.

Mrs. KELLY. Thank you very much.

My time is up. We turn now to Ms. Maloney.

Mrs. MALONEY. I would like to ask the Fed, Honorable Mark Olson, the white paper you discussed focuses on clearing and settlement. Are you planning a companion piece focusing on the areas that the GAO noted were left out? They cited trading and retail firms.

Mr. OLSON. A number of things have happened since the GAO study, or at least concurrent with the GAO study. Primarily among those was the release of an FFIEC best practices, that focused on those issues. So in addition to the clearing and settlement, there has been an internal effort within the regulatory agencies focused on the trading platforms and the retail platforms.

Mrs. MALONEY. I would like to ask the Homeland Security Assistant Secretary, Robert Liscouski, I understand that we were lucky in that the targets identified in the recent terror alert were not facilities whose destruction would pose a systemic risk to our financial structure. Rather, they were highly visible targets whose destruction would likely cause a large loss of life and have a symbolic value of attacking some of the most successful institutions in our financial services.

As you know, many of those targets are in cities. I would like to say that, especially New York City was cited in the last terrorist threat. Even worst, I believe, is that the facilities whose destruction would pose a systemic risk to our financial infrastructure are also largely located in major cities like the one I am privileged to represent, New York City.

My question is, how does this square with a formula for funding homeland security protections under which, to give one example, New York, according to the congressional survey, CRS report, ranks number 35? Yet in our area, certainly financial infrastructure, both the systemic structures that could cause disruption to our services, and certainly the ones that even the terrorists cite that are symbolic, are in New York City and other large places. So I wonder why this is happening? I commissioned a CRS study myself which showed that New York City has gotten about 30 cents per person for every dollar, and other states have received much, much more.

So just focusing on the infrastructure of our financial services, it seems incredibly unfair that New York City, which is cited by terrorists and also cited in intelligence briefings, is having the systemic structure that could really permit damage.

Mr. LISCOUSKI. Ma'am, I am not familiar with the results of the study you cited. I would be happy to get back to you with the exact dollars that have been distributed to New York City. I do not have that in my data here. I can tell you I am working with the New York City Police Department and the homeland security adviser in New York, as well as the private sector institutions. They have a very robust capability to respond to that threat.

As you well know, recently with the most recent threat situation we had in New York, the Department of Homeland Security as well as the New York City Police Department and the state police in New York responded very aggressively and very robustly to that particular threat. They were not impeded at all. We work very closely with the city in providing the appropriate level of resources they need to supplant their efforts. Again, I will get back to you in writing if you prefer, to respond to the exact dollar figures that have been provided. I just do not have that information.

Mrs. MALONEY. Even the 9/11 Commission report noted that the funding formulas for high-threat homeland security, they called it "pork barrel" politics, and certainly it should be based on need. I would appreciate your getting back to me.

Mrs. KELLY. Thank you very much. Ms. Maloney, your time is up.

Mrs. MALONEY. The light is not red yet.

Mrs. KELLY. Oh, I am sorry. I thought it was.

Mrs. MALONEY. Okay. I would like to ask Mr. Olson, did the events of 9/11 reveal a need for either new powers for the Fed or a need for new arrangements with the private sector, for example, foreign banks?

Mr. OLSON. Clearly, Congresswoman, we recognized that following 9/11 one of the most important things that we needed to have happen is that the Fed needed to be designated as an enforcement agency. That was accomplished in the Patriot Act. Congress responded very rapidly to that important need.

I think the response to 9/11 suggested to us is that there was a need to consider the risks at a level at which we had never considered them before, which is exactly what your opening series of questions was designed to get at, the most chilling of which was up to that point most business continuity plans were made presuming that the people would still be there. Post 9/11, that was the one thing that changed and the one thing that was different, and the one thing that we now anticipate seeing both from our own perspective and when we examine financial institutions.

The CHAIRMAN. [Presiding.] The gentlelady's time has expired.

The gentlelady from Illinois, Ms. Biggert.

Mrs. BIGGERT. Thank you very much, Mr. Chairman, and thank you members of the panel for your testimony and efforts to help America's financial sector prepare to withstand catastrophic events.

I am going to address my first question to Mr. Liscouski. I also am from Illinois, as the Chairman just said, and we do have concerns here about ChicagoFIRST. We will hear testimony later, so I do not want to say too much about it. I am concerned, and I would like to ask you what the Department of Homeland Security is doing to promote and encourage the infrastructure preparedness in the financial service sector, particularly with ChicagoFIRST,

which was a group formed by the financial sector in Chicago in the outlying areas after September 11.

I think the achievements that they have found in a regional way that they have to really have at their tabletop to have 27 financial institutions serving the City of Chicago, all of the agencies, the Federal Bureau of Investigation, Federal Deposit Insurance Corporation, FEMA, financial and banking information infrastructure.

What seemed to be missing there with all of these agencies was really the Department of Homeland Security stepping up to the plate and really being there for that, and to see how that works. Because I think that we see this as a model that can be used across the country. It seems that there has not been much support from the Department of Homeland Security.

Mr. LISCOUSKI. Congresswoman, thank you for your question. Actually, I would like to just add some more context to that, because I believe that since we have started up we have provided a lot of support to the financial sector, and particularly to the Chicago Mercantile Exchange and others where we have done tabletop exercises. So I think maybe a lack of initial visible support was just a function of the way we were starting up our organization.

Since that time, in the past year and a half, we have been working very closely with the sectors, particularly in the Chicago area. I think at the first tabletop, ChicagoFIRST was just standing up, so it might have been a little bit too early at that point. I can give you more details on that. But as you well know, working with Treasury and other members of the financial sector, we stood up at the Financial Services ISAC to conduct a number of tabletop exercises, all geared at the financial sector. We broadened the financial sector's tabletop exercises to not just include the cyber aspects, but now physical aspects. We are taking that on the road so we now can do more interdependent sector-type of tabletop exercises, just not uniquely those positioned for the financial services sector.

We are working very closely with the U.S. Secret Service, which is part of DHS as you well know. We have a very close working relationship with the investigative division of the U.S. Secret Service in remediating and working real-time on investigations and identifying various vulnerabilities in the financial sector, and quickly remediating those vulnerabilities in a virtual sense, working with banks and other financial institutions as they are found.

So while we have been building up our processes within DHS, I would remind you we have been around for about a year-and-a-half now. My department really was something that came up virtually with very little infrastructure of its own. As we have been building it and building partnerships, I think we have a very effective and very good story to tell there. So as I pointed out, we are funding many different types. These tabletop exercises are a prime way for us to be able to ensure that we have best practices and effective measures for protection of the financial sector.

ChicagoFIRST has been on our list now to work with. We understand that there is a request for some financing outside the FS-ISAC. We are working with them to examine that, maybe not as quickly as they would like at this point, but as in all things they do take some time, so we are examining those opportunities. I

would suggest to you that we will find ways that we continue to work with the financial sector.

Mrs. BIGGERT. I know that the testimony in the next panel will address those issues and say that they really have received no communication from the department as far as their inquiries into the funding, into procuring security clearances for key financial representatives, so that there can be a deeper collaboration. It seems to me that this does seem to be a real model, and I would hope that you would work closely with them and use them.

Mr. LISCOUSKI. Sure. I will take that under advisement and I will look into that specifically and get back to you. Thank you.

Mrs. BIGGERT. All right. Thank you.

And then Mr. Abernathy, certainly the Department of Treasury has been involved with ChicagoFIRST, too. Could you tell me a little bit about how you have worked with the ChicagoFIRST?

Mr. ABERNATHY. We certainly agree with you, Congresswoman Biggert, that ChicagoFIRST is a model to be taken around the country. We were involved with the ChicagoFIRST from its beginnings. In fact, one of my senior staffers is currently the head of ChicagoFIRST, Brian Tishuk. He was very much involved when he was working for Treasury in helping to get ChicagoFIRST organized.

But I want to give the chief credit to the financial community in Chicago that came together and realized that they have some very important national financial assets in that city that need protecting, and the best way to protect them is to coordinate efforts, to team up and to recognize that when it comes to protecting the financial infrastructure, it is not a matter of competition. It is a matter of coordination and cooperation.

What we are now in the process of doing is working together with the Financial Services Roundtable's BITS organization, another industry-coordinating organization, to document how ChicagoFIRST was put together, how it works, and put together what we call a cook book that we would then like to take to the other financial centers around the country and have them apply it as appropriate in those cities.

Mrs. BIGGERT. Thank you very much. I yield back, Mr. Chairman.

The CHAIRMAN. The gentlelady yields back.

The gentleman from Georgia, Mr. Scott.

Mr. SCOTT. Thank you very much, Chairman Oxley.

I have a couple of questions. First Governor Olson, in your testimony you stated that vulnerabilities continue to pose challenges to the financial system and that sound practices will be able to help recover from a widescale disruption. Yet you mention that sound practices addresses only recovery, and not prevention of a terrorist attack. I would like for you to talk about that for a moment, and particularly answer this question in light of that. Is the Federal Reserve currently involved with providing information or sharing information with law enforcement agencies to help prevent attack? What is the Federal Reserve doing in working with our other intelligence agencies to prevent the attack? Answer that one first.

Mr. OLSON. Sure. It is an excellent question and it gets to the heart of what we spend a great deal of our time doing. In the post-

9/11 era, we in particular have strengthened the resiliency. We have increased our focus on prevention. We begin with a premise that our number one priority is our people, so you cannot focus on your people without focusing primarily on prevention. So what we have done is we have looked at our perimeter security, and we have significantly upgraded both the quality and the quantity of our protection force, not simply at the Fed in Washington, but also throughout the Federal Reserve System.

We have increased our communication with law enforcement agencies and with other governmental agencies. We have monitored information carefully. The reason I bring that point up is because when we reviewed the information that was intercepted in the last several months, we have discovered how much information that was intercepted was information that was already on the public record. So we choose not to be real specific in a public forum. But you and other members of this committee are entitled to a lot more information on what we are doing, and we would be very happy to provide a private briefing for you on what we are doing in that area, because your questions are right on point. Much of what we are doing, particularly in the way of perimeter security, is involved in protection.

Mr. SCOTT. Thank you very much. I would be interested in that other detail.

Mr. OLSON. I have one more follow-up, because I would be remiss if I do not speak to it. The telecommunications area is one that we are still working on because of the interdependency of both the financial institutions and the interconnectivity among the private sector telecommunication companies. We are working jointly with that industry to try to assure a greater protective capability, but that is a subject which we will continue to focus on and hopefully the Congress will too.

Mr. SCOTT. Thank you, Governor.

Assistant Secretary Abernathy, in your testimony you said that most of the assaults on our nation's financial institutions are cyber attacks, computer viruses and organized crime. Could you share with this committee how those three areas impact our readiness for these terrorist attacks, organized crime, cyber attacks and computer viruses? And have you seen any evidence that terrorists have been sophisticated enough to mimic these types of attack? And how are they coordinating it, especially with organized crime?

Mr. ABERNATHY. Congressman, you have zeroed in on what I think is probably the number one area of concern and effort in terms of responding to existing vulnerabilities. We have done a good job as far as I think can be done with regard to the physical security. But with regard to the danger to the systems, the question is, what are the vulnerabilities to these cyber-attacks? As I mention in my testimony, we have seen them evolve from the pranksters into organized crime, and now we are beginning to see what we think is a pattern suggesting that it is going beyond organized crime to perhaps terrorists or others that are not interested in stealing the money so much as trying to keep the systems from operating.

We have been working very carefully with the financial institutions themselves, as well as the computer experts, the makers of

software, the designers of the hardware, and the designers of the systems, to create a more resilient system to respond to those kinds of cyber-attacks that might occur.

Mr. SCOTT. When you say "organized crime," are we talking about American organized crime? Are we talking about international organized crime?

Mr. ABERNATHY. It is both, sir. Now, American organized crime, but one that is particularly difficult to deal with is organized crime that originates from a foreign country. That is something that we have seen on the significant increase in recent months.

Mr. SCOTT. Okay. My last point was, if I could Mr. Chairman, very quickly, you also stated, Mr. Abernathy, that you sent a letter to the federal home loan banks to ask that they join the Financial Services Information Sharing and Analysis Center. Have you heard from these banks? If so, what have they said?

Mr. ABERNATHY. We have just recently sent the letter, so as we expect it takes time for them to process and make the decisions. We have asked the FS-ISAC, the financial services organization itself, to make the direct contacts to these banks and to ask them, you have heard from the secretary, the assistant secretary; you have heard from the chairman of the Federal Housing Finance Board; are you ready to sign on. We are very hopeful that they will, but we have not had any takers yet to this point, but it is still early.

Mr. SCOTT. Thank you.

Thank you for your generosity, Mr. Chairman.

The CHAIRMAN. The gentleman's time has expired.

The gentleman from Iowa, Mr. Leach.

Mr. LEACH. I am just trying to put a sense of perspective in what you are saying. It is impressive to me that a couple of words have come up. One is resiliency of institutions; another is redundancy of systems. It strikes me that the two R's are probably the most important concepts.

Just in terms of defense of our systems, I think we have to make it clear that decapitation does not bring us down. That is, loss of life, as Mr. Olson mentioned, is something that we are prepared to deal with in terms of how we proceed in the future.

My concern is that we have a dual circumstance, resiliency and redundancy in the private sector. We also have it in the public sector. In an emergency, the Fed is the center point. So I would like to ask Mr. Olson, are you confident of the Fed's resiliency and the Fed's redundancy of systems? While it was not designed for this purpose, does the fact that you have regional institutions magnify your strengths? Is decentralization also a systemic strength?

Mr. OLSON. Let me answer your questions in the reverse order of the one in which you asked them. In terms of the dispersal, the fact that we have Fed systems throughout the country is indeed part of our strength. It is part of our strength in terms of its role in monetary policy, but it also provides us with a physical diversity that is very important for us, while we are assuring both the resiliency and the redundancy. It meant that in many cases our ability to provide backup or partnering, the capability, the facilities were already there to do so. So that is particularly important.

In terms of our ability to meet future circumstances as they unfold, I think that the best way to respond to that is evaluating the manner in which we have responded in the past, for example to 9/11. I think the fact that the banking system did not close; that at no point in time did any customer even in Manhattan not have access to their personal financial information. Now, they might not have had access to the information at the branch or the ATM where they were accustomed to having it, but it was available because of the resiliency of the system and because of the large numbers of systems.

So I would say we are cautiously confidence. That is not a subject that we would ever take for granted.

Mr. LEACH. Is there such a thing as a Fed in a mountain?

[Laughter.]

Mr. OLSON. I am not sure what you are asking me.

Mr. LEACH. What I am saying is, do you have a second Federal Reserve headquarters?

Mr. OLSON. Oh. Could I get back to you on that on a private basis?

Mr. LEACH. Of course, fair enough.

Mr. OLSON. As with Congressman Scott, these are important questions that we would be happy to provide that information for you in another setting.

Mr. LEACH. Fair enough. Just one final, just to be very precise, the subject of Congress's approach to a possible bill on netting has been raised and addressed. I am correct in assuming that as Chairman Greenspan indicated in the last hearing, the Federal Reserve strongly supports a netting bill. Is that correct?

Mr. OLSON. Very much so. We appreciate your support and the support of the other members of this committee who have indicated their support for moving that bill. That would be a very important step forward, we believe.

Mr. LEACH. Treasury concurs?

Mr. ABERNATHY. Yes, sir. We would like to see that enacted either as part of the bankruptcy legislation or as free-standing legislation. It is very important.

Mr. LEACH. And our third witness, you would concur on that as well? Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. The gentleman's time has expired.

The gentleman from North Carolina, Mr. Miller.

Mr. MILLER OF NORTH CAROLINA. Thank you, Mr. Chairman.

My questions are about private sector preparedness and what we are doing to encourage it. The 9/11 Commission devoted a page to the topic. They pointed out that 85 percent of the critical infrastructure was in private sector hands. They said that they had encouraged the American National Standards Institute, ANSI, a very well respected industry group, to develop and promulgate national standards for preparedness, convening safety, security, business community experts, and to develop a voluntary national preparedness standard.

Mr. Liscouski, do you agree that those standards should be voluntary? Should there be some force of law behind them? Let me first disagree to some extent with Mr. Leach, who said that he

thought an attack on our financial institutions would be an act of barbarism, but not something that would bring our system down. It strikes me that a serious disruption in our financial institutions could have a catastrophic effect on our economy. Do you agree, first of all, that the risk is grave to our economy generally? And then second, that whatever standards we come up with, what we think the private sector should be doing, should be voluntary, as opposed to having some force of law behind it?

Mr. LISCOUSKI. Congressman Miller, I do not want to take this out of context, but I believe the statement regarding the catastrophic effect of the attack was the concern about the most recent threat.

Mr. MILLER OF NORTH CAROLINA. I was not referring to anybody else's testimony, then. I was talking about my own perception. I have attended a hearing on the Science Committee about the loss or disruption of the electrical grid. If that happened, the ripple effect through our economy could be very, very serious. It strikes me that the same thing is true in the financial services sector. If American business cannot get access to money, they cannot pay their bills, they cannot make payroll, they cannot buy materials. The people they do business with are not getting paid, and on and on. The possible loss there is serious. Do you not agree with that?

Mr. LISCOUSKI. Of course. In the broad context of what the overall catastrophic effect could be on the financial services in general, yes, that is exactly the type of thing we look at from the consequence-of-loss perspective. We always look at the consequence of loss when we are looking at sectors and vulnerabilities.

Mr. MILLER OF NORTH CAROLINA. Okay. How about the voluntariness? Do you think it should be voluntary or do you think there should be some force of law behind the standards that ANSI has promulgated, that the 9/11 Commission has said need to be abided by American business?

Mr. LISCOUSKI. I just want to conclude my previous comment by saying that we have yet to see, however, anything that would manifest itself in terms of a threat that would be at that catastrophic loss level. With respect to standards and regulation, as you well know the financial industry is fairly well regulated now. The standards that are imposed by the regulation in many cases adequately addresses the requirements to meet the specific threats that we are operating against.

I think in a general sense with respect to standards, we are looking to establish best practices and guidelines throughout the community, all the critical infrastructure components, to ensure that we get good compliance and practices to respond to various types of threat scenarios against which we are operating. Whether it be ANSI, we are currently working with the American Society of Mechanical Engineers to develop ways to bake into business processes for best practices. It is at that level that we think we can have the most benefit to affect the outcome of security for the long term.

I think the challenge in terms of looking at regulation or standards to remediate against a current threat, and they can never happen quickly enough. I think the best efforts we can make are looking for long-term systemic changes in business practices and security practices for the industry is irrespective in the financial

sector across critical infrastructure. My office in particular in working with the private sector to ensure that we take that approach.

The one thing we have to be very careful of is that there is not a one-size-fits-all standard. We have to be careful about ensuring that when we look at it.

Mr. MILLER OF NORTH CAROLINA. I am not sure I got an answer to my basic question of what should be behind it other than a hope for goodwill.

Mr. Abernathy, in your testimony you said the FBIIC will also try to share best practices, encouraging whenever possible, cajoling where necessary. That strikes me as a fairly limited range of options. First, we are going to encourage you, and if you do not do right, we are going to ratchet up and cajole you. I am not sure the prospect of being cajoled is going to strike fear in the hearts of a lot of folks. Is that your whole range of options, to encourage compliance with best practices or standards or whatever you call it?

Mr. ABERNATHY. Let me explain the context. The cajoling and encouraging is with regard to the federal and state regulatory agencies themselves. We do not have any enforcement authority with regard to the Securities and Exchange Commission, but the Securities and Exchange Commission, for example, has very significant authorities with regard to the entities that they supervise.

So when it comes to the encouraging and cajoling, it is making sure that the banking regulators, including the Fed, the SEC and other banking regulators are using their authorities to make sure that the financial institutions themselves are applying their regulatory powers and employing the kinds of best practices that you talk about, what the various standards are, to make sure that they are able to continue to provide the services that they are chartered to provide.

So the enforcement tools are in the hands of the regulators. The job of the FBIIC is to make sure that the regulators are using and applying those enforcement tools.

The CHAIRMAN. The gentleman's time has expired.

The gentleman from Alabama, Mr. Bachus.

Mr. BACHUS. Thank you, Mr. Chairman.

Governor Olson, I want to commend you. We talked about netting earlier, and I want to commend you and the Fed because Chairman Greenspan in some testimony before the Congress recently talked about how important the netting provisions were. So I hope the Senate gets the message, and we are able to include that in some legislation.

Mr. OLSON. We thank the members of this committee that have been supportive in that effort. We agree that it is important.

Mr. BACHUS. I would take this time just to say again that, Chairman Oxley, before 9/11 took steps which I think this committee, working with the regulators, to ensure that our financial institutions and our markets did go through 9/11 I think in an exemplary way.

My two questions I am going to ask are for Assistant Secretary Abernathy. You mentioned that $2 million that Treasury spent on the Financial Services Information Sharing and Analysis Center.

Mr. ABERNATHY. Yes, sir.

Mr. BACHUS. Can you tell me about what Treasury's commitment is to that center, which was formed actually by Executive Order?

Mr. ABERNATHY. The center itself was formed in 1999, if I am not mistaken.

Mr. BACHUS. Or 1998, by a presidential decision.

Mr. ABERNATHY. Yes. It was actually formed by the private sector pursuant to encouragement from the federal government, but it is a privately created and organized entity. What we did was in recent years, we looked at that entity that originally had a very narrow focus, coordinating the largest financial institutions. In visiting with them, we said in order to do your job you need to be able to reach all of the financial institutions. Of course, their response was, how do we do it?

So we funded a consulting group to look at just how you can expand the FS-ISAC and have it self-supporting. The FS-ISAC does not receive any operating funds from the federal government and we wanted to have a system that was sustainable by being funded by its members exclusively. We have come up with a plan and a reorganization that we believe is working and is moving forward very well.

Mr. BACHUS. What are your plans in regard to the future of the center?

Mr. ABERNATHY. It is to continue to have it develop as the central means of coordinating information among the whole financial sector. To demonstrate just how flexible it is, we have various levels of communication that are available on the FS-ISAC. There are first of all threat announcements that go out to everybody, but it is also a platform where specific segments of the financial sector can get together and communicate with one another on important critical infrastructure problems, and we are seeing already a number of efforts to do that and to use that as the platform for it.

Mr. BACHUS. Okay. Treasury provides critical financial services that need protection every day, like daily check forecasts and cash forecasts and collection and disbursement of federal funds or federal monies, conducting Treasury auctions, things of that nature. What are you doing to see that these important functions are somewhat insulated against potential threats?

Mr. ABERNATHY. You are absolutely right, Congressman. Besides being the chairman of these coordinating roles, Treasury itself has important roles in the financial system, particularly with regard to the movement of all the federal money, both the money that is coming in and then the money that is disbursed to pay all the bills and all of the checks. We frequently work with that element of Treasury in those particular bureaus to make sure that they have those two words that Congressman Leach talked about, resilient and redundant operations in place. We feel very confident that Treasury has those not only established, but we test them frequently.

Mr. BACHUS. All right. I have no further questions. I would like to say for the record, I think this is correct, the PDD-63 which President Clinton authorized and it was amended by Executive Order, but I think that mandated that the center be established. I could be wrong, but I am pretty sure that that would make sense because that was 1998, and if it was created in 1999.

Mr. ABERNATHY. Yes, I believe that is right. What I wanted to emphasize, though, is that it is a privately owned entity and we think it derives a lot of strength because of that, fostered by government, if you will, and encouraged, and it is built into a network of other ISACs. But its strength comes from the fact that it is owned and governed by the private sector.

Mr. BACHUS. Right. And I think we will see that in the second group of panelists who are some of the stakeholders or participants.

The CHAIRMAN. The gentleman's time has expired.

The Chair would announce we have about 8 minutes left on two floor votes. I would ask the gentleman from New York if he would be brief.

Mr. ACKERMAN. Brief.

The CHAIRMAN. That was the word I was looking for. The gentleman from New York.

Mr. ACKERMAN. Yesterday, the nation received very startling information from the Vice President of the United States. He contended that if he were not reelected, together with the President, and the Democrats instead were elected, that hundreds of thousands of Americans would be killed in a terrorist attack. I would like to know if that is a bunch of political hyperbole, or in the hard work that you have been doing at the Federal Reserve, at the Treasury Department, at Homeland Security, you have come across any information whatsoever, over the transom, rumors, chatter, or anything else that would indicate that there is any validity or truth to what the Vice President says.

Mr. OLSON. Speaking on behalf of the Fed, that is above my pay grade, Congressman. I do not have access to the information to answer it.

Mr. ACKERMAN. So you have seen no information that that is true?

Mr. OLSON. I would say that the question is above my pay grade. I have not addressed the question.

Mr. ABERNATHY. Congressman, I did not see the comments so I would not want to comment on it for my own. I will just add that we see constantly, as I have pointed out in my testimony, that the financial services sector is under assault every single day.

Mr. ACKERMAN. Nothing to do with Democrats?

Mr. ABERNATHY. As far as I can tell, it is a continuous assault that is not letting up in intensity.

Mr. ACKERMAN. Under a Republican administration.

Mr. ABERNATHY. This has been in place now happening for numbers of years.

Mr. ACKERMAN. But there is no indication that it is politically biased. Okay.

Mr. ABERNATHY. Nothing that I have seen.

Mr. ACKERMAN. And Homeland Security?

Mr. LISCOUSKI. I think my colleagues have perfectly addressed the question, sir. Thank you.

Mr. ACKERMAN. Has anybody made contingency plans just in case the Democrats are elected, in any of your agencies?

[Laughter.]

The CHAIRMAN. I have made some contingency plans.

[Laughter.]

Mr. ACKERMAN. I do not mean about your future personally. I thank the panel and I thank the Chairman for his indulgence.

The CHAIRMAN. Thank you.

Ms. Lee?

Ms. LEE. Thank you, Mr. Chairman.

Very quickly, let me just thank you again for being here. I come from the San Francisco Bay Area, and of course we are very concerned not only from attacks and vulnerabilities as it relates to natural disasters, but of course as it relates to vulnerabilities from terrorism.

I would just like to know what, as you see it in terms of the Bay Area, in terms of financial institutions, because many of the top financial institutions are in the San Francisco Bay Area, what do you see as some of the vulnerabilities?

What do you recommend, especially Mr. Liscouski, in terms of the coordination between federal, state and local officials in terms of the San Francisco Bay Area?

Mr. LISCOUSKI. Without getting into the specifics of the protective measures and the vulnerabilities, it is probably not appropriate for this forum, but I think I can talk generally speaking with respect to our coordination with state and local officials. We work very closely with the Homeland Security officials in California, and specifically the local officials in San Francisco, and routinely.

I would be happy to provide to you a separate reporting as far as what specific measures we have taken, again just out of deference for the type of information we are talking about.

Ms. LEE. Thank you.

Assistant Secretary Abernathy, what do you identify or have you looked at some of the greatest vulnerabilities facing San Francisco's financial district? Is that part of the overall planning that you have done?

Mr. ABERNATHY. One of the things that we do on a constant basis is trying to identify what are the key critical elements of the financial infrastructure; what their vulnerabilities are and then how we can address those. Certainly, we look at wherever they are. They are not located all in New York City. Some are there, and some are in other parts of the country. Financial services are extremely important to the economy of San Francisco and from San Francisco a lot of important financial services are provided throughout the nation.

One of the things that we think will be of great help to San Francisco and other money centers around the country is, as I mentioned, this cook book that we are putting together of looking at the ChicagoFIRST model and providing that to financial centers around the country and encouraging them to develop appropriate coordinating efforts in their cities as well.

The CHAIRMAN. The gentlelady's time has expired. We have to go to vote.

Ms. LEE. Okay. We have to go.

The CHAIRMAN. I want to just take the Chair's prerogative to ask Mr. Abernathy the status of TRIA, and just a few comments, then we have to close this down.

Mr. ABERNATHY. Certainly, Mr. Chairman. We are progressing as the law has outlined for us an analysis of how the Act is performing. We put in place, as I think we mentioned here previously, a very meticulous, sequenced data collection exercise so we could see just what is happening on the ground.

The CHAIRMAN. As required in the Act.

Mr. ABERNATHY. As required in the Act. We just received the most recent collection of data from insurance providers. We are also looking at developments not only here in the United States, but there is a very interesting development with connection to the Olympic Games.

There we had some very prominent activities that had absolutely no government support at all that were able to find terrorism risk insurance. We are looking at that example to see what it tells us with regard to the availability of the products.

The CHAIRMAN. I thank all of you, and this panel is dismissed. The committee stands in recess until 12 noon.

[Recess.]

Mrs. KELLY. [Presiding.] We welcome our second panel today. We have Mr. Robert G. Britz, president and co-chief operating officer of the New York Stock Exchange; Mr. John Mohr, chief operating officer, New York Clearing House; Mr. Wilton Dolloff, executive vice president, operations and technology, Huntington Bancshares Incorporated, on behalf of BITS and the Financial Services Roundtable; and Mr. Samuel Gaer, chief information officer, New York Mercantile Exchange.

Mr. Emanuel, I understand that you would like to introduce our next guest on the panel.

Mr. EMANUEL. Thank you, and thank you for holding this hearing.

I first went to meet with Brian and the ChicagoFIRST group a couple of months ago. Brian Tishuk is the executive director, and prior to that he had a distinguished career at Treasury working on a set of issues over there. ChicagoFIRST, in Brian's discussion and in answer to questions, will show as a role model to what other cities can do in a sense of the private sector coming together, starting ready-to-do planning to deal with unintended events.

In Chicago, like other major financial centers, we have about 320,000 to 350,000 jobs in the area who rely on the financial services industry, leaders in the future, it is an options industry. And what ChicagoFIRST has done is a remarkable job in coordination with also what the City of Chicago has done.

So I am pleased that the Chairwoman agreed to have ChicagoFIRST and Brian as a person to testify today. As I told Brian earlier, I have Alan Greenspan in the Budget Committee, and no disrespect intended, I am going to get and go there and ask my questions of Chairman Greenspan so I can tell Brian what interest rates are going to be like tomorrow.

I want to thank the Chairlady for holding this hearing and thank the entire panel for giving their time today.

Mrs. KELLY. Thank you very much.

Let us begin with you, Mr. Britz.

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

Mr. BRITZ. Thank you, Chairwoman Kelly.

Ranking Member Frank, distinguished members of the committee, I am Robert Britz. I am president and co-chief operating officer of the New York Stock Exchange. As such, I am directly responsible for the day-to-day operation of our market, our trading floor, our data-processing sites, our technical infrastructure, software development, and our information business. In addition, I also serve as the chairman of the Securities Industry Automation Corporation, or SIAC, which is a technology subsidiary of the New York Stock Exchange and the American Stock Exchange.

On behalf of the NYSE, I want to thank the committee for holding this hearing and giving us the forum to discuss the NYSE's investment in business continuity and contingency planning post-9/11. The NYSE lists more than 2,750 companies with a combined market capitalization of around $18 trillion. Just for context, the next-largest marketplace in the world hovers between $2 trillion and $3 trillion. We trade on average 1.5 billion shares a day, or in dollar terms about $50 billion. Ensuring the world's largest equity market can open for business every day under all circumstances is clearly our highest priority.

Madam Chairwoman, the NYSE has a long history of developing forward-looking business continuity strategies that harden and protect our physical and 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 vis-a-vis visitors and deliveries. Business continuity planning did not begin after 9/11. Before 9/11, we made sure that all of our facilities had emergency generators, uninterrupted power supply, and stored water on-site, to enable continued operation after the potential loss of power or water.

Our technology infrastructure was already connected to a private extranet that utilizes geographically redundant fiber routes. The NYSE and SIAC 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 technology complex 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. Since September 11, the NYSE has made an investment totaling more than $100 million to prevent and/or recover from an interruption to our market. The specific business continuity programs include both new initiatives, as well as enhancements to existing programs. In particular, the NYSE has built a contingency trading floor, expanded SIAC's emer-

gency command center, created the Secure Financial Transaction Infrastructure network or so-called SFTI network, constructed a remote network operations center, and recently received approval to establish a remote national market system data center.

The NYSE's regulatory group filed and the SEC recently approved new business continuity rules, Rule 446 for NYSE-member firms. In addition, beyond ensuring the resiliency of the NYSE, to ensure continuity of trading the NYSE has modified its systems to accept four-character symbols so that we can be a position to trade over-the-counter Nasdaq securities should that ever be necessary.

In addition, we have enhanced NYSE and SIAC disaster recovery planning, physical and information security; developed and implemented a mandatory business continuity training program for all NYSE and SIAC employees; enhanced emergency employee communication systems to ensure key personnel can be reached; and all personnel have access to relevant and timely information in an event. We have instituted a temporal dispersion initiative with respect to the data center staff, and we also are adding additional generating capacity at the New York Stock Exchange proper.

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

The NYSE and SIAC launched the Secure Financial Transaction Infrastructure network, or SFTI, as I mentioned a moment ago. It has become the primary extranet serving the financial industry. It provides diverse redundant routing to SIAC data centers for member firms, national market system participants that are connected to the NYSE, to the American Stock Exchange, the National Market System, and DTCC's IT infrastructure as well.

Following 9/11, 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 near ground zero. SFTI addresses this by enabling member firms to connect to the NYSE's data centers via multiple access points, so-called carrier hotels throughout the New York metropolitan area, as well as Boston and Chicago. From these access centers, message traffic is carried over a geographically diverse fiber network owned and managed by SIAC.

Beyond the resiliency of our market, the NYSE is prepared to trade Nasdaq stocks if that case ever arises. While NYSE systems have been modified and can support four-character symbols used by the unlisted stocks, no need for any modification on the part of the broker-dealer systems. And because our capacity today, NYSE's capacity vis-a-vis its own stocks, is about five times our average daily volume of 1.5 billion shares, we have no question about the ability to absorb the extra traffic resulting from Nasdaq stocks.

Madam Chairman, in your invitation to testify this morning, you also asked that the NYSE share its experiences relative to the limited code orange threat issued on August 1. On Sunday, August 1, Secretary Ridge of the U.S. Department of Homeland Security announced that al Qaeda was targeting specific sites in Washington,

D.C.; Newark, New Jersey; and New York City, including the NYSE. In addition, Secretary Ridge announced that the Department of Homeland Security was raising the terror threat level to orange for New York City. At approximately 6 p.m. the prior evening, the New York office of the FBI contacted NYSE security officials to inform them that the FBI had information that was very pertinent to the NYSE, and they requested that we meet with them immediately, which indeed we did.

This intelligence clearly indicated that al Qaeda had surveiled the NYSE. On Sunday, August 1, the FBI and the NYPD informed the NYSE that there would be immediate increase in NYPD officers and NYPD "Hercules" teams deployed around the NYSE's perimeter. In addition, the NYPD would increase the number of truck inspections for vehicles traveling south of Canal Street to determine if those trucks actually needed to proceed downtown toward the financial district.

On Sunday, August 1, the NYPD pledged their assistance for police department access and cooperation during the heightened alert. The Department of Homeland Security, as well as other federal, state and local agencies, notified the NYSE before Secretary Ridge's announcement that the exchange was a specific target. With this advance notice, the NYSE was able to communicate with its employees through our contingency Web sites. Under these contingency sites, we are able to provide timely information about the status of our operations for Monday, August 2, to members, member firms, member firm employees, and NYSE employees.

On Tuesday, August 3, NYSE officials met with Homeland Security Secretary Ridge, New York City Mayor Michael Bloomberg and both pledged their cooperation in the provision of federal and New York City assets as needed.

Since 9/11, all of our efforts have served to increase the NYSE's physical security, presence, and its business continuity planning. Our enhanced business continuity contingency planning are online and being tested every day. Unlike many localities and sites, New York City and the NYSE remain at a higher level and will remain at a heightened alert to protect the people and the infrastructure that operate the NYSE's agency-oriented market.

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 confidence to America's 85 million investors. While the NYSE and SIAC have implemented a comprehensive contingency plan that will provide for an orderly resumption of trading in the event of an attack or other catastrophe, we cannot prepare for every possible contingency. We will continue to work with the SEC, the Department of Treasury, Homeland Security, and the NYSE's member firms, the financial services industry, and federal, state and local law enforcement to address the threats and to implement strategies and solutions.

I hope the foregoing is helpful to the committee. We look forward to working with this committee going forward on matters of mutual interest, and I would be happy to answer any questions. Thank you.

[The prepared statement of Robert G. Britz can be found on page 65 in the appendix.]

Mrs. KELLY. Thank you so much, Mr. Britz.

Mr. Mohr?

STATEMENT OF JOHN MOHR, EXECUTIVE VICE PRESIDENT, NEW YORK CLEARING HOUSE

Mr. MOHR. Good afternoon. My name is John Mohr and I am an executive vice president of The Clearing House, which is headquartered in New York. Just to correct the record of the cover sheet of the testimony, it lists me there as the chief operating officer. I wish that I were, but I am not.

Mrs. KELLY. Thank you.

Mr. MOHR. We are headquartered in New York and we are the nation's oldest and largest clearinghouse. We are owned by 19 very large, global, international and regional banks. We were founded in 1853, and we are a private sector global payments system infrastructure that clears and settles more than $1.5 trillion each day. We serve as an industry forum for addressing strategic and regulatory issues dealing with payments made in U.S. dollars. The Clearing House serves more than 1,600 U.S. financial institutions and manages payment services that span the entire spectrum of paper, paper-to-electronic, and electronic payments.

I want to thank you for this opportunity to update you on steps we have taken to further strengthen the key elements of the U.S. payment infrastructure which are operated by The Clearing House. One of the key lessons learned from the 9/11 disasters was that from a business continuity perspective business as usual was no longer adequate. Contingency and business continuity plans needed to be reevaluated and refocused.

Since 9/11, the financial industry has increased its focus on the resiliency of its high-value payment systems. It is universally agreed that systems such as CHIPS, which is our large-value payment system, must be capable of resuming full capacity operations quickly, within hours of any catastrophe. We take this responsibility seriously. It is worth noting that CHIPS never skipped a beat on 9/11 and the days that followed.

CHIPS itself operated without interruption during the entire crisis and all 56 banks that connect to it were able to continue to conduct business. This included the 19 banks that were located in or near the World Trade Center. Each of these banks was required to relocate their operations to contingency sites in the middle of an unimaginable disaster. The fact that this was successfully accomplished I believe is a great testament to the leadership in these banks.

Following 9/11, our management reviewed the events of the week for lessons learned. Some of the things that we have done, we added additional security staff to perform more frequent and random patrols of our facilities. We conducted penetration tests of both our physical security and our logical security for our systems. We reconfigured one of our facilities to make it better prepared to prevent penetration. We implemented state-of-the-art biometric access controls. We also all but eliminated visitor access to all of our operating centers.

We reviewed where our critical employees worked and relocated some of these individuals to avoid a concentration risk of having

too many key individuals in one place. We have taken measures to ensure that key operations and support staff have secure remote access to our electronic systems so that they can operate remotely in the event that they cannot get to our principal operating centers. For many years, The Clearing House has operated fully redundant data centers, each with the capability of backing up the other. To further enhance its resiliency, we have developed and out-of-region third data center. This new center is fully equipped to take over the operation of CHIPS within an hour of a simultaneous failure of the other two sites.

One key procedure which was reaffirmed during the events of 9/11 is contingency tests. Mandatory testing of contingency capabilities has been conducted by CHIPS since the early 1980s. The tests cover a variety of disaster scenarios and exercise the backup and recovery capabilities of the participants, as well as CHIPS. The performance of each participant during these tests is evaluated by The Clearing House and those banks that fail the test are required to continue to re-test until they pass. The discipline of regular testing helped contribute to the quick recovery of the banks following the events of 9/11. Since 9/11, we have expanded our own testing regimen to include two tests a year, coordinated with the Federal Reserve's Fedwire system.

Another significant initiative led by the Clearing House following the events of 9/11 was our Intercept Forum which addressed the question, what could financial institutions, working with the public sector, do to eliminate the flow of funds to terrorists and their organizations. We had senior representatives from 34 public and private sector organizations. This forum identified five task groups which were co-led by representatives from both the public and private sectors. These five groups, let me touch on them briefly: patterns of behavior, account transaction monitoring, and global cooperation.

The first three I think are easily understood, their purpose, their mission clearly understood by the names of their groups. The other two, control list, following the events of 9/11, the banks and the regulators and the law enforcement agencies needed to sit down and clarify what we were trying to accomplish in terms of identifying terrorists, flows of funds to terrorists, what policies and procedures had to be in place, what new was being put in place. All this had to be communicated effectively, so we put a group together to work on that.

Our fifth group, a database team, was originally set up to develop a highly secure real-time capability to download suspected terrorist information and to upload hits that financial institutions may have, reporting them back to the law enforcement agencies. This fifth group was superseded by FinCEN and their PAC system which was set up in 2003, I believe. We work closely with them and handed over that responsibility to them. All of our banks have been working with them since.

I think the Intercept Forum is a great example of the private and public sector's ability to work together to achieve shared goals. Financial institutions, law enforcement agencies, and regulators were able to draw upon each other's core competencies in a cooperative way and achieve meaningful results. It is clear that going forward

we will need continued cooperation in all three areas to be successful.

Thank you.

[The prepared statement of John Mohr can be found on page 116 in the appendix.]

Mrs. KELLY. Thank you.

Mr. Dolloff, I understand that Mr. Tiberi was wanting to come to introduce you because you were a fellow Ohioan. I hope you will take my introduction, from being a former Ohioan who now is in New York. We are delighted to have you here. You may proceed.

STATEMENT OF WILTON DOLLOFF, EXECUTIVE VICE PRESIDENT, OPERATIONS AND TECHNOLOGY, HUNTINGTON BANCSHARES INCORPORATED, ON BEHALF OF BITS AND THE FINANCIAL SERVICES ROUNDTABLE

Mr. DOLLOFF. Thank you, Madam Chairman and members of the committee for this opportunity to testify about the financial services industry's efforts to address critical infrastructure protection. I am Wilton Dolloff, executive vice president for operations and technology at Huntington Bancshares, Incorporated. I am pleased to appear before you today on behalf of BITS and the Financial Services Roundtable. I have submitted a written statement that provides details on efforts by BITS and the financial services industry to strengthen our nation's critical infrastructure.

I would like to use this time today to deliver three messages. First, the financial services industry is doing an outstanding job strengthening our slice of the critical infrastructure pie. Among other things, we have developed emergency communication tools, conducted worst-case scenario exercises, engaged in partnerships with the telecommunications sector and key software providers, compiled lessons-learned from the 9/11 attacks and the August 2003 blackout, and combated new forms of online fraud.

Second, as you know, our industry is heavily regulated. The regulators have stepped up their oversight, but we cannot address these problems alone. Our partners in other sectors, primarily telecommunications, power, software, must also do their fair share to ensure the soundness of the nation's critical infrastructure.

Third, I want to review several recommendations for the Congress to consider. Since 9/11, our sector has done a lot to respond to the risk we face today. Protecting our nation's critical financial services infrastructure is a top priority. I would like to highlight several efforts to help assure the security stability of our sector.

We have improved communications and enhanced our ability to analyze and disseminate information. For example, we have enhanced the financial services information sharing and analysis center, the ISAC, providing an important tool for members to share and analyze cyber and physical threat and vulnerability information. In addition, we have established the BITS-FSR crisis communicator. This high-speed alert system rapidly notifies CEOs and CIOs and others as appropriate to convene conference calls during which industry leaders share information and make decisions. The system was recently activated on August 1 immediately following the threat-level escalation by the Department of Homeland Security for the financial industry.

One of the key lessons learned in recent years is our sector's dependence on other critical infrastructure sectors, namely telecommunications and power. BITS is working with the telecommunications industry to identify and mitigate vulnerabilities and enhance recoverability. While the cooperation between these two sectors has been unprecedented, much more work remains to be done.

In August 2003, the blackout occurred in the Northeast. It gave us an opportunity to test our assumptions about what would happen in a large-scale loss of power. In general, the financial services industry performed well. Backup systems operated. Alternate communications systems were used and there was no measurable impact on settlements and payments.

Our industry has also been working hard to strengthen cyber-security. We have stepped up our efforts by sharing information, analyzing threats and working more closely with the software industry. In December 2003, BITS surveyed its members on the cost of addressing software vulnerabilities and learned that costs are approaching $1 billion annually. In February 2004, BITS and the Roundtable held a cyber-security CEO summit to launch efforts to promote CEO-to-CEO dialogue on software security issues.

In short, we want the software industry to improve the security of products and services that they provide to us. Just as financial institutions are key targets for hackers and other cyber-criminals, our industry is increasingly the target of fraudsters operating online. We are responding to the escalation in identity theft with a series of steps to facilitate prevention of the crime and assist victims when it occurs. The cornerstone to these efforts is the BITS-FSR Identity Theft Assistance Center, or ITAC. The concept of this pilot program is to provide a simplified recovery process that benefits victims by relieving much of the current burden of reporting the theft and restoring one's financial identity.

The Congress can help the financial services sector meet the challenge of the post-9/11 environment in three ways. Number one, encourage the telecommunications industry to provide diverse and reliable services to critical infrastructure sectors. Two, recognize the dependence of all critical infrastructures on the software operating systems and the Internet. And finally, number three, encourage law enforcement to prosecute cyber-criminals and identity thieves and publicize U.S. Government efforts to do so.

I am pleased that Congress has an active interest in helping to shore up the financial sector against vulnerabilities and hope that we can work together to heighten security. Financial firms will continue to work diligently to achieve the level of security that our customers demand.

Madam Chairman, I will be happy to answer any questions. Thank you.

[The prepared statement of Wilton Dolloff can be found on page 86 in the appendix.]

Mrs. KELLY. Thank you so much.

Mr. Gaer, we welcome you.

STATEMENT OF SAMUEL GAER, CHIEF INFORMATION OFFICER, NY MERCANTILE EXCHANGE

Mr. GAER. Thank you, Madam Chairwoman. Good morning, and thank you to the members of the committee for inviting me to address the issue of emergency preparation and vigilance for the financial services sector. The subject matter is of timely concern and I sincerely welcome the opportunity to both express what the New York Mercantile Exchange has accomplished to date, as well as to express concerns regarding areas in which you might consider providing assistance to our efforts going forward.

The Exchange is the world's largest physical commodities futures exchange and has been an example of market integrity and price transparency throughout its 132-year history. Commercial enterprises and government entities all over the world use our marketplace to manage their energy metals risk, a function that is particularly critical to the global economy in any time of crisis. The Exchange is also a technology leader in the futures industry, developing robust, redundant, best-of-breed trade management clearing and reporting systems capable of quick fail-over to backup systems when required.

No preparedness planning, however, can be accomplished without a careful analysis of the business that needs to be protected. Our core business is trading and clearing. In order to ensure the continuity of this core business, we have pursued several alternatives. The Exchange headquarters was designed to be as redundant as possible, including the availability of backup generators, which became critical during the blackout of 2003.

One of the first priorities for the Exchange after September 11, for example, was to build a replica trading floor which contains trading rings, administrative space, live price feeds, and a fully operational and redundant data center. In other words, it is a complete facility. This facility has been powered-up since the beginning of the Iraq War and is ready to go on a moment's notice.

The Exchange also has two electronic trading systems, both of which have round-the-clock trading capability. In fact, we were the first exchange in New York to reopen following September 11 when we opened our electronic trading system for a 2-hour session on September 14, which resulted in a record 70,000 contracts being traded in 2 hours.

During an emergency, the high-level strategic decision-making authority rests with the crisis management team which we call the CMT. It is comprised of members of the executive committee of the board of directors, C-level executives and critical senior executives. Their role is to assess a threat and if necessary provide an official declaration of disaster, to interface with the members of the exchange, and to coordinate with industry and regulatory agencies.

Maintaining communication between recovery units and resources is the single most important aspect of any emergency recovery effort. The Exchange has gone to great lengths to ensure that the CMT and their subordinates are all able to communicate, including provision of cell phones with two-way radios, mobile e-mail devices, laptops with cellular modems which we affectionately call footballs, and access to CFTC-sponsored GETS cards. Every critical exchange system is duplicated and can provide services in

the event the main facility or system is unavailable. Data moves across redundant optical fiber links, linking our backup site to the primary site. In addition to the network created between the two hot sites, the Exchange maintains multiple links to Internet service providers.

Training, education and regular testing will ensure that the systems and staff are ready to respond to any event that disrupts our business. Ongoing planning for events keeps the Exchange planners in top form. The Exchange, along with the Futures Industry Association, or the FIA, have begun planning a major multi-company and multi-exchange coordinated testing effort which will culminate in the first annual industry-wide disaster recovery test this fall on Saturday, October 9. The effort is extremely important to our industry and will be repeated annually.

As a critical infrastructure organization, we strive to learn from every event we face. So what were the lessons we learned from the various events that we have handled recently? The tragic and cataclysmic events that took place on September 11, 2001 showed us that planning for emergencies that involve a single company, building or service is no longer adequate. As we look back at 9/11, the relationships the Exchange has forged with government agencies will always be of critical importance in planning for and support during an emergency event. In addition, the relationships our member firms have formed with important government leaders have enabled the Exchange to overcome many difficult recovery challenges in the past.

The blackout of 2003 taught us different lessons, foremost of which is that the unavailability of a facility is not a prerequisite to an emergency event. Multiple redundant service providers need to be secured for all critical business services. Other events that the Exchange planners carefully consider are the planning we have done for the Republican National Convention and the regular disaster recovery testing and mock disasters that the Exchange conducts all serve to reinforce and fine-tune the planning we have at the ready. Communications stands alone as the key equalizer when facing the surprises any emergency delivers. A disaster gives no advance warning.

Madam Chairwoman, in closing I ask this committee to consider the following concerns from the Exchange. As an integral part of the critical infrastructure, the Exchange already manages a full complement of continuity plans, backup sites and emergency operation locations. However, our business relies upon the coordination of many services within the financial sector. It also relies heavily on telecommunications, utility and transportation infrastructure over which the Exchange has no control. The Exchange is prepared to recover our systems and business processes if faced with another event such as 9/11, but the recovery of the services and the price discovery mechanisms we provide to the financial services sector and economy also relies on resiliencies of the external businesses on which the Exchange depends.

I would like to thank the Chairwoman and the members of this committee for inviting the Exchange to speak with the other distinguished panelists on this extremely important topic. I would be happy to answer any questions the committee has.

[The prepared statement of Samuel Gaer can be found on page 101 in the appendix.]

Mrs. KELLY. Thank you very much, Mr. Gaer.

Mr. Tishuk.

STATEMENT OF BRIAN S. TISHUK, EXECUTIVE DIRECTOR, CHICAGOFIRST

Mr. TISHUK. Good afternoon. Chairman Kelly, members of the Financial Services Committee, I am Brian Tishuk, the executive director of ChicagoFIRST, a coalition of 16 of Chicago's leading financial institutions. A list of our members and government partners is appended to my written statement.

Through ChicagoFIRST, these institutions cooperate with one another and collaborate with government to address common business continuity and homeland security issues. This ensures that our business continuity and disaster recovery plans conflict neither with one another nor with the government's plans for prevention, response and recovery.

In light of the events of September 11, the Chicago financial community, as others, reexamined and enhanced their individual business continuity plans. During the spring and summer of 2003, a number of these institutions also decided to form ChicagoFIRST. Two leaders took it upon themselves to commit their time and their respective firms's resources to make this coalition a reality: Louis Rosenthal, executive vice president at LaSalle Bank and Ro Kumar, first vice president at the Options Clearing Corporation.

From the beginning, our top priority was to get a seat in the city's Joint Operations Center or JOC. The JOC is a place where different government agencies, city agencies, come together to address a crisis, whether it is a snowstorm or a terrorist attack. We sought a seat to ensure access to accurate and timely information in case of an emergency. We obtained this seat in July of 2003. Our members are also working with the city and the state to learn where our respective evacuation procedures may conflict and to take remedial action.

Another absolutely critical objective for the financial community in Chicago is credentialing. ChicagoFIRST and the city are using an interim credentialing solution that we put together with them, while the city and the state together develop a permanent one. ChicagoFIRST is also working with the city and the Red Cross to develop shelter-in-place protocols. These best practices will protect our members' employees at the office and their families at home.

Now, every regional partnership will necessarily be unique. However, ChicagoFIRST has been constructed in a manner that would allow its salient elements to be replicated in other parts of the country. I would like to highlight four components of our model. First, financial institutions should organize themselves in a grassroots fashion and leadership should come from within the financial community. Second, with the critical infrastructure largely in the hands of the private sector, we have an obligation to put some "skin in the game," as the saying goes. However, at least in the short term, funding from the public sector should also be provided.

Third, information sharing is key. Such sharing ranges from the mundane of my calling the city to find out why there are a number

of police cars and fire trucks outside a particular building, to the absolute essential of having the city and state give us a heads-up about impending issues and announcements such as the August 1 disclosure of terrorist threats against financial institutions on the east coast. Finally, not only can the above elements be replicated elsewhere, but also adapted to any region, even outside of financial centers where other sector participants may be necessary.

I would like to mention briefly the crowning achievement of 2004, a July tabletop exercise that proved successful in every way. Most importantly, we devised a scenario that examined how the partnership would function if financial institutions were forced to operate for an indefinite period of time under the threat of terrorist attack. Unfortunately, 2 weeks after the event, we saw that very scenario unfold in real life on the east coast that allowed us to be ahead of the game in Chicago.

In conclusion, the members of ChicagoFIRST are very proud of our progress. While much remains to be done, Chicago's financial community is better prepared to protect its employees and businesses than it was before ChicagoFIRST was formed. We hope that our successful approach can provide a model for private-public partnerships in other cities throughout the country. Thank you again for the opportunity to testify at this important hearing, and I am happy to answer any questions the committee may have.

[The prepared statement of Brian S. Tishuk can be found on page 136 in the appendix.]

Mrs. KELLY. Thank you, Mr. Tishuk.

I would like to ask a couple of questions, but before I do three of the five members of this panel are from New York and participated in the recovery. I want to compliment all of you. You were back up. You were functioning. Our financial systems in New York were functioning so quickly. You are to be complimented for the work that you did prior to 9/11 to ensure that that actually happened.

I would like to begin with asking a general question, actually, but I am going to focus this on you, Mr. Britz. The Stock Exchange has often been thought to be a target for terrorists. In the press, it was indicated that terrorists had cased the Exchange as a potential target. In a broad sense, what additional steps have you taken since you heard about people casing the place?

Mr. BRITZ. First of all, I will share with you an anecdote, Congresswoman. When we met, I referenced in my remarks, we met with Homeland Security, we met with the FBI the evening before, the Saturday evening as a matter of fact, and the NYPD and a number of local law enforcement agencies. We asked them point blank, what can we do, what might we do that we are not now doing? The answer uniformly was, nothing; that they regard what we do today or what we did prior to the most recent announcement as the gold standard.

They, in turn, again as I referenced in my remarks, the NYPD in particular supplemented their force on the ground around our perimeter both in terms of patrolmen, but also in terms of the Hercules swat team, if you will, so that we had a very substantial presence over and above what we normally have. I know you have seen

what we normally have, so I think it is the gold standard. But post-9/11, essentially what we did was push out our perimeter.

We had well before 9/11 magnetometers, X-rayed every package, every valise. I myself walk through a magnetometer every morning. My briefcase goes through the X-ray every morning. But that, of course, is once you are inside the building. We pushed the perimeter out, as you know, with the help of the NYPD so that you cannot get within a block of the Stock Exchange with a vehicle without going through a checkpoint, having canine sniff, checking the manifest, having the dog sniff as to whether or not there is any explosive capability and so on. So essentially what we have done and what we have reinforced with the help of the police department is to extend that external perimeter away from the building.

Mrs. KELLY. Thank you.

I know there are a number of people who enjoy the fact that now there is a sense of a mall around the Stock Exchange. It certainly is pleasant to be able to walk without having to worry about the traffic down there.

Mr. BRITZ. Those are the people who are not in vehicles.

[Laughter.]

Mrs. KELLY. Right. Exactly.

Mr. Dolloff, you represent BITS. I asked a question of Mr. Liscouski in the earlier panel. I do not know if you were in the room. I am very concerned about the insider threat with regard to the programs that are in each one of the businesses that work in the financial industry. I am concerned about them because I understand that it is possible for people in the process of the programming and reprogramming to fit the niche market that each business needs, there are programmers who are there who are doing certain things.

Is there something that you can tell me that the industry itself, from your BITS organization, the BITS FSR is doing, to perhaps profile the people who are doing programming, to do some kind of a check so that the programs do not yield up information that might be essential information to people that we actually would rather not have that information?

Mr. DOLLOFF. Congresswoman, if I understand the question correctly, I would like to address it from the Huntington's perspective first, because I am not sure of the organization efforts of BITS in this area. I can tell you that many financial institutions have programming standards and oversights over their programmers. One person may develop a program and it then goes through a testing process, and what we call a "change control" process where people outside the unit that did the program, review the program for its legitimacy and to make sure that it is doing as it is intended to do.

Now, is it possible for somebody to be so clever that it could sneak by even that checkpoint? Probably. You can only protect against what you think you know. But I think that is a standard that you will find in most financial services industry shops, if you will, on how they control the quality of the programs that they develop.

Mrs. KELLY. My concern is that so many of us look at a threat from outside, hackers, people like that. My concern is the threat from inside.

Mr. DOLLOFF. I would agree with you. There is always a threat, both externally and internally. As I said, we need to make sure that we have these dual checks in place, and sometimes it is more than dual checking. They go through very extensive testing processes to make sure that the program development that has taken place does what it is intended to do.

Mrs. KELLY. My time is up. I do have a few more questions, but I am going to turn this over now to Mr. Miller.

Mr. MILLER OF NORTH CAROLINA. Thank you, Madam Chair.

I wanted to pursue a question that I began with the first panel about compliance in the private sector with the necessary safeguards against terrorism; that 85 percent of our infrastructure is in the private sector. There has been apparently a fair amount of effort to try to develop standards.

Mr. Britz, you referred to the New York Stock Exchange's standard as the gold standard, which I commend you for, but I am afraid that a great deal of the private sector will not adopt a gold standard, but a tarnished brass standard of going cheap on terrorism safeguards, when in fact they are at risk and there are consequences beyond. There are consequences to their employees. There are consequences to anybody else who may be on their premises. And there are consequences to the people that they do business with, in a ripple effect.

The 9/11 Commission recommended a voluntary standard. Any of you, do you agree that it should be voluntary? Or should there be some force of law behind some standard in the private sector for terrorism safeguards? We can start with you, Mr. Britz, and work our way down.

Mr. BRITZ. First of all, Congressman, when I referenced a gold standard, it was the New York City Police Department and the FBI referring to us, not us referring to ourselves. It was in the area of physical security.

Mr. MILLER OF NORTH CAROLINA. Either way, I commend you.

Mr. BRITZ. Gosh, I really do not feel confident to address that question other than to perhaps offer a private sector comment which would be that it is in the private sector's interest to safeguard their respective franchises. I know that the New York Stock Exchange has done everything it has done, even though we are overseen by the Securities and Exchange Commission to be sure, and the word "cajole" was used earlier. They cajole us every now and again.

But most, if not everything that we have done in the area of protecting our infrastructure has been self-initiated because it is in our business and our franchise interest to do that. So you have that kind of a motivator resident within every private sector business that has assets and franchises to safeguard.

Beyond that, I am not a regulator of the banks or the paying agencies and so on, and I do not know if I would comment beyond that.

Mr. MILLER OF NORTH CAROLINA. Anybody else? Try to keep it fairly brief because I only have 5 minutes. Yes, sir?

Mr. MOHR. Yes, I would agree with most of what Mr. Britz said. I think it is in the interests of the private sector to make sure they are safe and sound. I would also point out that the regulators, in my opinion, did an excellent job following 9/11, leading the review on an industry-wide basis and coming up with a lot of good clear thinking, good clear direction.

I think the partnership between the two was essential to making us as strong as we are today. I think the best way forward is to keep that partnership going, keep driving the two together to make sure that they are working together.

Mr. MILLER OF NORTH CAROLINA. Anyone wish to speak up for something other than a volunteer standard? All right.

A second point that the 9/11 Commission made, let me read one question, their bolded recommendation: "We believe that compliance with the standards should define the standard of care owed by a company to its employees and the public for legal purposes."

I took that to be a reference to the substantial body of state negligence law, of common law negligence of what the standard of care is, and that reference means that they believe that under state common law businesses that did not adopt the appropriate safeguards, and there are consequences to others as a result of their failures, should give rise to civil liability.

There is also a wealth of economic theory that says that the civil liability system is a market mechanism to assure proper safeguards. Do you agree that the civil liability system would apply in cases, certainly now that we know there is a terrorism threat, to the consequences of a failure to take appropriate safeguards? Anybody want to stick up a hand? Mr. Britz, do you want to start with you?

Mr. BRITZ. Congressman, I apologize. I do not feel confident to respond to that question. I am neither a lawyer nor an expert on what it is the Commission intended in those words.

Mr. MILLER OF NORTH CAROLINA. Okay.

Mr. Mohr, do you have any comment?

Mr. MOHR. I have nothing to add to that.

[Laughter.]

Mr. MILLER OF NORTH CAROLINA. Mr. Dolloff?

Mr. DOLLOFF. I would agree. I do not feel qualified to answer that question.

Mr. MILLER OF NORTH CAROLINA. All right.

Mr. Gaer?

Mr. GAER. I would also agree. I am neither a lawyer nor an expert on what you are reading.

Mr. MILLER OF NORTH CAROLINA. Mr. Tishuk?

Mr. TISHUK. I am afraid it is not my area of expertise either.

Mr. MILLER OF NORTH CAROLINA. Okay. I am pleased that I was able to bring about so much unanimity among the panel.

[Laughter.]

Mrs. KELLY. Thank you very much, Mr. Miller.

Ms. Biggert.

Mrs. BIGGERT. Thank you, Madam Chairman.

I would like to congratulate all of the members of this panel for their self-initiated efforts to bolster the infrastructure of America's financial sector, and to take the offensive approach in that.

I would especially like to applaud you, Mr. Tishuk, not just because you live in Homer and are a constituent, but for what you have done with ChicagoFIRST in providing a model partnership between the public and private sector in this area.

Could you just tell us a little bit more about the tabletop and what happened and why that is so important, and what you learned from it?

Mr. TISHUK. Certainly. The tabletop took place in mid-July. We had terrific participation, some 17 government agencies, 21 financial institutions, telecommunications providers, power, water. It included all of the relevant areas of the city and the state, as well as the federal government. It was very useful.

The whole object of the tabletop was to assess assumptions that we all had about one another, to make sure that we knew what we could really expect from one another during an emergency, rather than finding out something we did not expect in the heat of the moment.

It certainly provided a lot of grist for our mill. Everybody has told us it was very successful, that they learned a lot about all the other participants. We certainly learned a lot. We learned our communications systems are even more fragile than we had initially thought, and we are working to find alternatives to the conference calls that we tend to rely upon.

We are also reaching out to the counties surrounding Chicago, because our employees come from there and we certainly learned more about the city's and state's evacuation plans for getting folks out of the city, out of Cook County and beyond. Therefore, it is important to make sure that they are part of this dialogue so that our employees know what they can expect to find if such an event occurs.

Perhaps most importantly, given its success, we learned that it is very much a goal for us to test, implement lessons learned to fill the gaps, and repeat, both in the table top format, which is somewhat artificial, as well as in a testing mode where you are in your office or where you are supposed to be normally, and then respond.

Mrs. BIGGERT. It was mentioned earlier, or it was mentioned in your testimony that you have had trouble communicating with the Department of Homeland Security, while you have worked very closely with the Treasury Department. Do you think that that will change after today?

Mr. TISHUK. I certainly have that expectation, yes. I would like to point out, though, that we have had excellent support and a relationship with DHS's regional arms in Chicago. Both FEMA and the Secret Service have been with us every step of the way. They have been forthcoming with their ideas and very supportive to our suggestions. So from that standpoint, things could not be better.

Mrs. BIGGERT. One of your suggestions has been that you would have a regional center for the Department of Homeland Security in Chicago.

Mr. TISHUK. Correct. Chicago is a vital center. As the East Coast hardens for good reasons, we certainly want to make sure that terrorists do not look upon Chicago as a softer alternative to attacking financial institutions and metropolitan areas.

Mrs. BIGGERT. Thank you for all that you do.

I have another question for probably most of the people on the panel. After 9/11, a number of financial firms managed to shift trading and portfolio management to their offices in London and other financial capitals. Should major global financial institutions include in their disaster recovery plans the ability to shift trading and book management temporarily away from the affected country? Do some of you have that in your plan in case that there is a disaster? Mr. Britz?

Mr. BRITZ. I will take a shot at that, Congresswoman. In our Rule 446, the business continuity rule, and I am now talking about broker-dealer member firms of the New York Stock Exchange, we impose a requirement that they demonstrate the ability to operate under various circumstances, but we do not dictate as to how.

When you say "shift away" from the affected country, and this country is a fairly large country, that may very well include shifting to other centers that they may have literally around this country, as opposed to necessarily going to Europe or some other center. The NYSE as a regulator of broker-dealers dictates that you have to demonstrate the capability, but we do not dictate as to how.

Mrs. BIGGERT. Mr. Mohr?

Mr. MOHR. For the commercial banks, the regulators have already told the larger banks that they must have certain recovery capabilities that are outside the immediate region. That process is already under way, but there is no directive that they have to move offshore. Those banks that did move offshore did so because they are multinational banks that have processing centers in other areas of the world.

Mrs. BIGGERT. Mr. Dolloff?

Mr. DOLLOFF. I would agree with what Mr. Mohr just said. We have backup facilities outside our immediate region. We, however, are not an international or have an international presence, so we would not have that capability to go outside the United States, but we do have backup facilities.

Mrs. BIGGERT. Mr. Gaer?

Mr. GAER. Like everybody else on this panel, our business is intensely competitive. In an event such as 9/11, for example, let us call it a sister exchange of hours. We got a phone call from somebody across the pond to host their book, and that was their biggest fear, if you will, because they felt that once that liquidity goes offshore, it is going to stay there.

As such, we do have a fully redundant trading facility where if we needed to move trading, we could move trading to that facility. We have two separate, fully redundant electronic trading systems that if the facilities are not available, we can use those facilities. We in the midst right now of looking at actually globalizing and providing a presence offshore as well.

Mrs. BIGGERT. Thank you.

Mr. Tishuk?

Mr. TISHUK. You raise an important issue, but it falls outside the scope of our particular mission.

Mrs. BIGGERT. Okay. Thank you. Thank you all.

I yield back.

Mrs. KELLY. Thank you, Ms. Biggert.

One thing I did want to just mention, Mr. Gaer you said that you are dependent on the external infrastructures. I simply want to offer this committee's help, if you have some ideas of things that we might be able to do. You can certainly call my staff. We would be very interested to do whatever we can for you, because I realize that you are in many ways affected by that more than some of the other people involved in financial services.

Gentleman, I neglected to say as you sat down that without objection, your written statements will be made part of the record. You have been recognized for 5-minute summaries of your testimonies, but your testimony will be made a part of the record, your full testimony.

The Chair notes that some members may have additional questions for this panel which they may wish to submit in writing. So without objection, the hearing record will remain open for 30 days for the members to submit written questions to these witnesses and to place their responses in the record.

We thank you very much for your patience and for your testimony today. This hearing is adjourned.

[Whereupon, at 1:15 p.m., the committee was adjourned.]

A P P E N D I X

September 8, 2004

Prepared, not delivered
Opening Statement

Chairman Michael G. Oxley
Committee on Financial Services

"Protecting our Financial Infrastructure: Preparation and Vigilance"
September 8, 2004

Saturday will mark the three-year anniversary of the terrible attacks of September 11. All of us remember that day and the dreadful uncertainties it brought.

Our nation's financial-services sector was able to withstand the stress and was quickly operational again. Much of the credit for that goes to the individuals who work in the industry, who spent countless hours to make sure that our nation's commercial lifeblood kept flowing with little or no interruption. Credit also goes to the business-protection and business-interruption planning and investment that began in the late 1990s as the nation prepared for the Y2K rollover.

While the quick recovery of U.S. market operations demonstrated the resilience of the American financial system, 9/11 exposed a laundry list of vulnerabilities. Though the loss of life and the physical destruction of the World Trade Center buildings were the most immediate consequence of the attacks, the threat to computer systems, telecommunications networks, electrical power grids, transportation systems, the paper check-clearing system and even water supplies supplying climate-control and computer-cooling systems was real.

We all know that those attacks may not be the last to rattle our country or our financial sector, and that potential business interruption may result from natural disasters — a hurricane, for example. Large catastrophic events like the train fire in Baltimore that severed a major East Coast telecommunications link, or the cascade of events that blacked out a large portion of the Northeast on August 14 of last year are also a serious consideration.

In the years since 9/11, the government and the private sector have worked unceasingly to strengthen the infrastructure that is critical to the functioning of our financial system. That infrastructure ranges from the physical, buildings that house banks and exchanges and clearing operations, to the computers that store and manipulate the data that is the lifeblood of our financial system, to the electrical power that runs those computers and the telecommunications lines along which that data runs.

Improved information-sharing, between industry and government and within the industry, has developed and refined "best practices" of protection and of business-resumption techniques.

Of course, efforts to protect the financial sector's critical infrastructure, like efforts to protect the country itself, can never cease. What was good enough as a protection against threats yesterday, must necessarily change tomorrow as the nature and type of threat changes. Intentional or accidental computer viruses and denial-of-service attacks by definition will be different tomorrow than today. Terrorists are determined and creative, and the risk of accident is always present.

Domestic efforts to strengthen our critical infrastructure are the first best defense. But America's leading role in the global financial system requires us also to keep an eye on how vulnerabilities abroad can affect our markets. Threats to our financial institutions and international financial organizations can emanate from anywhere and be transmitted through the Web. We need to be able to distinguish between terrorist threats and more fraud-oriented hacker threats. Both are serious, but they require different response mechanisms. Within the private sector, ensuring that counterparty relationships and back-up liquidity facilities exist in the event of extraordinary threats to the marketplace are critical components of a security plan as well as good business practice.

From that perspective, the limited, industry-specific and location-specific raising of the terror threat level, issued August 1 by Homeland Secretary Ridge, offers us an excellent illustration of the evolution of this process of protecting our critical financial infrastructure and the international organizations that are located in our country. Instead of raising the threat level for the entire nation, affected institutions and locations were alerted nearly instantly, as our witnesses will tell us today. The result was increased watchfulness where it was necessary, without undue anxiety or the unnecessary use of resources where it was not.

As the world becomes increasingly complex, and as financial markets become increasingly global and inter-related, I am glad we have dedicated public servants, and smart, hard-working folks in the private sector focused on this issue. We have several of them here today as witnesses to tell us how far we have come in the protection of our critical financial infrastructure, what we must yet do, and how Congress can help.

OPENING STATEMENT OF CONGRESSMAN SPENCER BACHUS
FULL COMMITTEE HEARING
"PROTECTING OUR FINANCIAL INFRASTRUCTURE: PREPARATION AND VIGILANCE"

Thank you, Mr. Chairman, for convening this important hearing on protecting our nation's financial infrastructure. Under the leadership of Chairman Oxley, this Committee has conducted ongoing oversight of preparedness, incident-recovery and critical infrastructure protection issues going back to the pre-Y2K period, and with greater frequency since the attacks of 2001. I want to thank the Chairman for holding this hearing today and commend him for playing a substantial role in ensuring that our financial infrastructure is protected from terrorist attacks and natural disasters.

September 11th taught us that our nation's financial infrastructure could withstand a major attack. Even though the nerve center of our financial system was hit hard, our financial markets were up and running several days after the attack. Nonetheless, September 11th also exposed our major weaknesses. We all saw the devastation of the World Trade Centers but the attacks also brought down computer systems, telecommunications networks, electrical power grids, transportation systems and even water supplies.

Since that time, other incidents have further demonstrated the need constantly to refine and upgrade safeguards to the financial infrastructure. On August 14th, 2003, numerous power-company generator and transmission failures culminated in a massive blackout in parts of New

York, Connecticut, Pennsylvania, New Jersey, Ohio, Michigan and southern Canada. Major hurricanes have caused widespread destruction and power outages in Florida and the mid-Atlantic states.

Since the September 11th attacks, this Administration has vigorously implemented strong measures to protect our nation's financial infrastructure from terrorist attacks and natural disasters. Most recently, Department of Homeland Security Secretary Tom Ridge warned of possible al-Qaeda terrorist attacks against "iconic" financial institutions, saying a confluence of detailed intelligence pointed to the serious threat of a car or truck bomb attack. In an unprecedented action, the government named specific buildings as among the potential targets and raised the threat level to Code Orange for the financial services sector in New York City, northern New Jersey, and Washington, D.C. Secretary Ridge's warnings prompted local, state and federal officials to protect these sites and take appropriate steps to ensure the safety of the employees of these financial services companies.

Let me close by welcoming Governor Olson, Assistant Secretary Abernathy and Assistant Secretary Liscouski. I look forward to their testimony and the testimony of our other witnesses at today's hearing.

I yield back the balance of my time.

Statement of the Honorable Rahm Emanuel
Committee on Financial Services
September 8, 2004

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

It's my privilege to introduce Brian Tishuk, Executive Director of ChicagoFIRST. I appreciate Mr. Tishuk taking the time to be with us today, and I look forward to his testimony about how the ChicagoFIRST model can be replicated across the country.

ChicagoFIRST is a dynamic, cutting edge organization and a model for how regional public/private partnerships can enhance the resiliency of financial institutions. ChicagoFIRST was founded because of the foresight of the Chicago's financial services community, and it succeeds because of the cooperation and encouragement of the public sector, especially the City of Chicago and State of Illinois.

Like other major cities, Chicago has a diverse financial services industry employing thousands of employees and serving as a key regional economic growth engine. A disruption of Chicago's financial markets for any extended period would do untold damage to the local economy and to equity, futures and options markets around the world.

After September 11th, several of Chicago's financial institutions decided that it would be mutually beneficial to partner with other private sector and government entities. The result has been a successful regional partnership that has shared ideas, conducted exercises, implemented contingency plans and learned valuable lessons that the members are eager to share with their counterparts across the nation.

Although he's been with ChicagoFIRST for just a few months, Mr. Tishuk has already made a significant impact. He came to ChicagoFIRST after a distinguished career at the U.S. Treasury Department during which he addressed an array of public policy issues affecting financial institutions, from the savings and loan crisis in the mid-1980s to the September 11th attacks.

Recently, I had the opportunity to meet with Brian and ChicagoFIRST co-chairs Louis Rosenthal of LaSalle Bank and Ro Kumar of the Options Clearing Corporation to see their fine work firsthand.

As a former Board member of the Chicago Mercantile Exchange and investment banker, I know firsthand the need to protect critical financial infrastructure, and I'm thankful for the groundbreaking work ChicagoFIRST has done to protect the financial services infrastructure in my hometown.

I thank Brian and ChicagoFIRST for their efforts, and I look forward to his testimony.

Thank you, Mr. Chairman.

September 8, 2004

Opening Statement by Congressman Paul E. Gillmor
House Financial Services Committee
Full Committee Hearing entitled "Protecting our Financial Infrastructure: Preparation and Vigilance"

Thank you, Mr. Chairman, for holding this important hearing and for your continued leadership in protection for our critical financial infrastructure. This Committee acted swiftly in investigating the economic impact of market closures and other results of the devastation of September 11, 2001 and has worked with both government and private sector officials to develop and implement policies to ensure our economic security in times of crisis.

Just last month, we were warned by Homeland Security Secretary Tom Ridge of possible al-Qaeda terrorist attacks against several financial institutions, naming specific buildings in New York City, northern New Jersey, and Washington, DC as potential targets. Many of us heard on the nightly news of additional security measures that were taken by the responsible police departments, including the closing of streets, limiting access to bridges and tunnels, and increased identity verification procedures. I am interested to hear from our distinguished witnesses this morning on the reaction of our financial system, both our regulators and the financial institutions involved, to these specific threats.

Our U.S. markets demonstrated their strength and resiliency in the quick recovery that followed September 11, 2001 but vulnerabilities were also shown. I am interested to learn more today regarding the cooperation between the Department of Homeland Security, Federal Reserve, Treasury Department and industry executives in the initiatives addressing such concerns and going forward.

Two years ago, this Committee requested the Government Accountability Office (GAO) to undertake a comprehensive examination of the preparations that financial market participants have taken since 9/11 to protect themselves from physical and electronic attacks. Last year the GAO produced a report that recommended additional steps to be taken by financial market participants to protect themselves from further attacks. I would

like to revisit those recommendations today and hear what steps have been taken toward their implementation.

Thank you again, Mr. Chairman, for calling this timely and important hearing. I look forward to an informative session.

OPENING STATEMENT OF THE HONORABLE RUBÉN HINOJOSA
HOUSE FINANCIAL SERVICES COMMITTEE
"PROTECTING OUR FINANCIAL INFRASTRUCTURE: PREPARATION AND VIGILANCE"
SEPTEMBER 8, 2004

Chairman Oxley and Ranking Member Frank,

Thank you for holding this very important hearing today.

The United States needs to remain prepared for any and all terrorist attacks following the horror that we endured on 9/11.

We need to remain vigilant to ensure that similar attacks never happen again on U.S. soil.

As I noted during the Committee's hearing on the 9/11 Commission Report during the August recess, we here in the United States need to focus on increasing the security of our own documentation, such as driver's licenses, passports and visas in order to prevent such terrorists from entering the United States again.

9/11 Commission Vice Chairman Lee Hamilton agreed that we need to increase the security of our own documentation, and such measures should include requiring biometric information and security features such as fingerprints, digitalized photos, holograms, and serial numbers, on these types of documents and increasing the technology with which financial institutions can verify IDs.

Prior to 9/11, the only United States consulate that required biometric information from individuals seeking entry into the United States was the U.S. consulate in Mexico. Such biometric data, and more, is now included as part of the twelve security features Mexico added to the matrícula consular ID card in 2002. As the Washington Times noted some time ago, the updated matrícula consular ID card as of 2002 is more secure than many U.S. documents.

Perhaps we should emulate the security features incorporated into the card as we create a new, more secure system of documentation in the United States.

The United States was very lucky that the 9/11 terrorist attacks did not completely halt the free flow of the U.S. capital markets for very long.

Granted, the New York Stock Exchange and others closed down for a time, and certain Federal Reserve Bank airplanes were unable to fly for a time due to the flight restrictions following the terrorist attacks.
These Federal Reserve flights are an integral part of the payment clearinghouse system in the United States.

I was very impressed by the ability of the New York Stock Exchange to adapt quickly to the terrorist situation and to accommodate the trades of so many exchanges on its own system in the days following 9/11.

Since 9/11, the NYSE, other exchanges, brokerage houses, and other entities have put into place systems to ensure that the capital markets will continue to operate at alternate sites if terrorists attack again.

Furthermore, I am pleased that Congress passed the "Check 21" legislation. That legislation facilitates electronic check imaging and authorizes the use of "substitute checks," a paper reproduction of the original check.
Today, I hope to learn from today's witnesses what measures they are taking to protect our financial infrastructure, to ensure business continuity as well as to determine if Congress needs to take additional action to protect our financial infrastructure from terrorists.

Mr. Chairman, I yield back the balance of my time.

Statement of Congresswoman Sue Kelly
"Protecting our Financial Infrastructure: Preparation and Vigilance"
September 9, 2004

This morning, the Committee convenes to continue its ongoing oversight of preparedness, incident-recovery and critical infrastructure protection issues. I thank Chairman Oxley for holding this hearing.

At the heart of critical infrastructure is the safety and soundness of the financial services sector, which drives every aspect of our economy. Earlier this Congress, the Oversight and Investigations Subcommittee held a hearing to examine the state of readiness of the financial services sector and the critical infrastructure that allows it to serve our country. In that hearing, the Subcommittee learned about the many promising steps that have been taken by our financial caretakers, as well as the constant assessments and improvements that still must be performed.

Over the last several years, our country has experienced many extraordinary events that have threatened the safety of the American people and our financial system – from the horrific attacks of September 11, 2001 to other blackouts and hurricanes. Fortunately, our markets have experienced remarkably quick recoveries, illustrating the tremendous resiliency of our financial system and the U.S. economy.

As a result of these events, it is apparent that the technology age we live in – which allows us to provide services and access information in a heartbeat – is both a boon and one of our greatest vulnerabilities. It is imperative that we continually revise our efforts to protect data systems and the infrastructure that allow them to operate, which are evermore intertwined and dependent on one another. Today, this review could not be anymore timely.

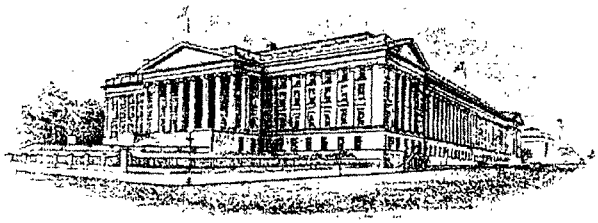
Last month, Department of Homeland Security Secretary Tom Ridge issued a warning of possible al-Qaeda terrorist attacks to our financial institutions, including Prudential Financial, the Citigroup Center building and the New York Stock Exchange, as well as the International Monetary Fund and World Bank buildings. The Committee is very interested in the steps that have been taken to protect our financial infrastructure since the threat level was elevated to Code Orange for the financial services sector in New York City, northern New Jersey, and Washington, D.C.

As terrorists continue to target our economy and financial institutions, we must ensure our financial infrastructure is strong enough to withstand diverse attacks. We must ensure that all of our systems – whether financial, energy, transportation or telecommunications – are able to operate under any extraordinary circumstances.

The Committee is pleased to have with us Federal Reserve Board Governor Mark Olson who has been a leader in these efforts in his role at the Fed. We also welcome the Assistant Secretary for Financial Institutions at the Treasury Department, Wayne Abernathy, who also serves as the Department's sector coordinator for critical infrastructure protection. Also joining us is the Assistant Secretary of Homeland Security for Infrastructure Protection, Robert Liscouski, who is responsible for the Department's efforts to identify our critical infrastructures and propose protective measures to keep them safe from terrorist attacks.

Keeping our financial systems functioning and safe requires a high degree of coordination between many different and important parties – both public and private. The Committee is also pleased to have with us witnesses on our second panel who are leaders in protecting critical financial services assets from major disasters – including several individuals from the Great State of New York. These witnesses, along with others in the private sector and government who could not be represented here today, are working in the field every day to protect our financial system.

The Committee thanks all of our witnesses for your appearance here today, and we look forward to your testimony. Together we can ensure that our financial systems are functioning smoothly under all circumstances and that the American people have full confidence in the financial services sector.



DEPARTMENT OF THE TREASURY
OFFICE OF PUBLIC AFFAIRS

EMBARGOED UNTIL 10:00 AM
September 8, 2004

Contact: Brookly McLaughlin
(202) 622-2960

Testimony of
Wayne A. Abernathy
Assistant Secretary of the Treasury for Financial Institutions
before the
Committee on Financial Services
United States House of Representatives

Wednesday, September 8, 2004

Introduction

Chairman Oxley and Ranking Member Frank, thank you for inviting me here today to testify on the progress of the financial services sector and the government in promoting the security and resilience of the nation's critical financial infrastructure.

I am pleased to tell you that the financial services sector is in an advanced state of readiness and preparation, and that it handled well the receipt of the recent information about terrorist targeting of specific financial institutions. No trading or financial activity was disrupted as a result of the recent threat elevation to Orange for the financial services firms in New York City, Northern New Jersey, and Washington, D.C. Customers were able to continue their business as usual. While there was concern, there was no crisis. There was no panic but rather activation of planned steps to mitigate exposure to risks. I congratulate the participants in the financial services sector for their actions, and especially for their excellent preparation, and I applaud our intelligence and law

enforcement agencies for obtaining this vital threat information and promptly sharing it with the affected institutions.

Organizing to Protect the Critical Financial Infrastructure

President Bush has led the development and implementation of an effective program to defend our country against terrorism. Protection of our financial infrastructure is a key element of that program, and much valuable work has already been done. That is because we have long known in general what recent information has reaffirmed with specificity, that our financial institutions are being targeted by our enemies.

The threat is not theoretical. Our nation's financial institutions are under assault virtually every day. Most of these assaults are in the nature of electronic or cyber attacks, such as computer viruses, Trojans, worms, and various forms of financial fraud, including phishing and spoofing. These assaults have progressed from computer hackers and pranksters, into theft, and now we believe on to schemes to disrupt the operations of our financial systems. Some of these attacks have their sources in organized crime. We believe that, increasingly, still more sinister actors are involved. I do not say this to be alarmist but rather to make the point that our financial institutions have for some time now been operating in a dangerous environment and are becoming increasingly adept at doing so successfully.

This success has not come easily, but as a result of careful organization and hard work on the part of the private sector and government agencies at all levels, federal, state, and local. The organized government effort is today based upon a directive from President Bush, Homeland Security Presidential Directive 7 (HSPD-7), which institutionalizes the national policy and overall framework for federal departments and agencies to identify, prioritize, and protect the critical infrastructure and key resources of our country. This is a flexible, coordinated program that works well in marshaling resources and activities in an organized fashion, agile enough to adjust to changed circumstances. HSPD- 7 places upon the Department of Homeland Security the central responsibility for coordinating the overall national program for critical infrastructure protection. While doing so, the Directive avoids reinventing the wheel, relying upon specific agencies to take the immediate lead—within the system of overall coordination by the Department of Homeland Security—thereby ensuring that critical protection efforts will continue to be led by departments that have the particular, sector-specific expertise and experience. The Department of the Treasury is the lead agency for the banking and finance sector and continues in that role under HSPD-7.

This arrangement has been tested several times in recent months and works well. I want to take a moment to commend Homeland Security Department Assistant Secretary Liscouski in particular for making this arrangement successful in practice, for ensuring that interagency cooperation has crowded out any opportunity for institutional rivalry. He has been and is a great partner, and we appreciate his efforts and those of the

dedicated men and women who work with him in the Information Analysis and Infrastructure Protection Directorate at DHS.

An important insight that informs the Administration's strategies is that nearly all of the financial critical infrastructure is owned by the private sector. As President Bush stated, "it is important to remember that protection of our critical infrastructures and key assets is a shared responsibility. Accordingly, the success of our protective efforts will require close cooperation between government and the private sector at all levels."

Not surprisingly, therefore, we work very closely with the private sector, and we do so on a cooperative, coordinated basis. This cooperation and coordination are made possible through reliance upon several private sector organizations. Chief among these is the Financial Services Sector Coordinating Council (FSSCC), the Chairman of which is the financial services Sector Coordinator, appointed by the Secretary of the Treasury. The current Sector Coordinator and Chairman of the FSSCC is Don Donahue, Chief Operating Officer of Depository Trust & Clearing Corporation and President and COO of both The Depository Trust Company and National Securities Clearing Corporation, two subsidiaries of DTCC. The FSSCC is made up of entities and trade associations representing virtually every financial institution in the nation.

Alongside the FSSCC is the Financial Services Information Sharing and Analysis Center (FS-ISAC), an industry created and supported network that serves as the chief communications system for the financial services sector on a wide variety of threats and challenges to its members. Treasury has played an important role in significantly expanding the activities and membership of the FS-ISAC, so that it can meet the communication and coordination needs of financial firms of all sizes. Last year Treasury devoted $2 million to develop and implement a plan for restructuring the FS-ISAC, the results of which have been very encouraging. In the last couple of weeks, Federal Housing Finance Board Chairman Alicia Castañeda and I sent a joint letter to each of the Federal Home Loan Banks, encouraging them to join the FS-ISAC, and we continue our outreach efforts to encourage all financial firms to sign up.

Federal and state financial agencies are similarly organized and their activities coordinated to promote the security and resilience of the financial system. Under the sponsorship of the President's Working Group on Financial Markets, the Financial and Banking Information Infrastructure Committee (FBIIC) brings together all of the federal financial agencies as well as representatives of the state financial supervisors. Specifically, the FBIIC is chaired by myself, the Treasury Assistant Secretary for Financial Institutions, and includes representatives from the Commodity Futures Trading Commission, the Farm Credit Administration, the Federal Deposit Insurance Corporation, the Federal Housing Finance Board, the Federal Reserve Board (as well as the Federal Reserve Bank of New York), the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Federal Housing Enterprise Oversight, the Office of Thrift Supervision, the Securities and Exchange Commission, and the Securities Investor Protection Corporation. In addition, state financial supervisors participate in the FBIIC through representatives from the Council of State Bank Supervisors, the North

American Securities Administrators Association, the National Association of Insurance Commissioners, and the National Association of State Credit Union Supervisors.

A cardinal rule of the FBIIC and a key to its success is the principal of responsibility. The FBIIC relies upon each agency to bear the full weight of its field of responsibility. The FBIIC does not try to take over that responsibility or interfere in the work of each agency in carrying out its statutory mandates. What the FBIIC provides is a means of coordinating those efforts, sharing best practices, pooling talents and resources, facilitating communication, encouraging wherever possible, cajoling when necessary. The Treasury Department has the role of orchestrating and facilitating this central service.

Some of the actions that Treasury has taken in recent months include the following:

- Arranging for critical financial institutions to have access to priority telecommunications services—both land-based and wireless—to help their voice and data communications get through during times of crisis.

- Assisting in coordinating the protective response of state and local authorities with critical financial institutions in their communities.

- Establishing systems and procedures that enable the federal financial regulators to communicate among themselves and with the private sector during times of crisis as well as in advance efforts to mitigate risks to the financial infrastructure.

- Conducting or sponsoring numerous tests, drills, and exercises to ensure that back up systems work and that financial professionals know what to do in times of either a heightened alert or an actual attack.

- Upgrading the Financial Services Information Sharing and Analysis Center (FS-ISAC) with financial assistance for new technology as well as for the development of a more inclusive business model that embraces all elements of the financial sector. This next-generation FS-ISAC now delivers integrated physical and cyber alert information to thousands of financial institutions and provides a secure, confidential platform to help financial institutions respond to potential or actual disruptions.

- Establishing a plan for working with the telecommunications, energy, information technology, and transportation sectors to address vulnerabilities introduced into the financial sector by interdependencies with these other sectors.

Recent Focused Elevation of the Threat Level

Our nation's enemies have shown themselves to be adaptive, innovative, and persistent. In the recent response to the threats against specific financial institutions we

have demonstrated that we have become even more adaptive, innovative, and persistent, ready to cope with a changing threat environment.

While the threats themselves are bad news, I see much good news in our latest experience. I am pleased to report that during the recent elevation of the threat level to code orange for New York City, Northern New Jersey, and Washington, D.C., the system created for promoting the security of our critical infrastructure has been working. Our anti-terrorism efforts are bearing fruit, providing valuable information, and that information is being applied and acted upon appropriately by the financial sector just as soon as it is made available, without disruption or degradation of services. This recent information was shared with the targeted institutions, with state and local governments, and with appropriate federal agencies. Treasury worked closely with DHS, coordinated activity within the FBIIC, and harmonized interaction with the FSSCC and through the FS-ISAC.

The response by the targeted financial institutions, and the financial sector as whole, was impressive. Action was immediate and business like. These institutions were able to use the information provided by the government to make informed decisions about the best course of action to take to protect their employees, customers, and the institutions themselves. They knew what to do because they had planned and prepared to address potential threats or disruptions. By and large, they implemented plans prepared well ahead of time.

Of course, the success does not lie in the plans themselves so much as with the people who developed and implemented them. I cannot say enough about the talent and dedication of the men and women of the financial services sector—in the private firms and in the public agencies. They deserve the thanks of those of us who use their services, and that includes just about all of us. Notwithstanding the threat information—that they had to view as alarming—these people energetically set to work to make sure that their protective measures and plans were implemented, and that the services they provide to their customers would continue without interruption. As I have said before this Committee and in outreach efforts around the country, our first priority is and must be people. And observing that priority works.

As a final point, in connection with the war on terrorism, the success of the collective actions of the federal, state, and local governments, and the preparedness and response of the private sector to promote the security and resilience of the financial sector, are progressively denying terrorists of their objective—their goal of disrupting our free markets. Freedom and free markets are the targets of the terrorists, and we are showing that we can harness the power of free people and free institutions to defeat the terrorists. There is much work yet to do, but tremendous work has already been done. Our markets are deeper, more resilient than ever before, and they are becoming more so every day.

This Congress and your Committee have been deeply interested and constantly supportive of this effort. Last year I reported to Chairwoman Kelly and the Oversight

Subcommittee on the financial sector's response to the power blackout. I had a good report to make then. I am pleased to report today that the financial sector continues to make progress, and we look forward to your continued interest, oversight, and support as we work on the tasks ahead.

Robert G. Britz

President and Co-Chief Operating Officer

New York Stock Exchange, Inc.

On

"Protecting our Financial Infrastructure: Preparation and Vigilance"

Committee on Financial Services

United States House of Representatives

Washington, DC

Wednesday, September 8, 2004

Introduction

Chairman Oxley, Ranking Member Frank and distinguished Members of the Committee, I am Robert G. Britz, 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, technical infrastructure and software development and information business. In addition, I serve as the Chairman of the Securities Industry Automation Corporation ("SIAC"), the NYSE's technology subsidiary.

On behalf of the NYSE and our Chairman John Reed and Chief Executive Officer John Thain, I thank the Committee for providing this forum to discuss the NYSE's investment in business continuity and contingency planning since September 11, 2001.

The NYSE lists more than 2,750 companies with a combined market capitalization of approximately $18 trillion. The NYSE trades an average of approximately 1.5 billion shares each day and the average daily dollar volume is approximately $50 billion. Ensuring that the world's largest equities market can open for business every day is one of the NYSE's highest priorities.

Business Components

There are seven critical business components required for NYSE trading:

1. The NYSE's Trading Systems - located in separate, active data centers that are designed to recover and resume trading intra-day after the loss of a data center;

2. The NYSE's Trading Floors – a primary Trading Floor and a backup Trading Floor. 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 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 – Securities member firm and specialist personnel; and
7. Clearance and Settlement Processes - these systems are hosted and operated by both SIAC and the Depository Trust Clearing Corporation (DTCC).

September 11, 2001

The attacks of September 11, 2001, will be ingrained in our national memory forever. The NYSE was not spared. Three of our members and hundreds of our member firms' employees were killed. Thousands of others were displaced. The attack on the World Trade Center hit particularly close to home, since the NYSE's Enforcement Division was housed in the South Tower. Fortunately, all of the employees in the Enforcement Division escaped safely.

Despite the loss of life and the terrible destruction that took place literally at our doorstep, the NYSE never lost the capability to trade. With our own emergency generators available for use, and most of our systems located off site and on a separate power grid, we had the capacity to continue to offer investors all the services that they have come to expect from the world's

premier equities market. If the business of the Exchange was dependent solely on those who directly participate in the auction process on the Trading Floor, we could have resumed trading earlier.

On September 12, 2001, a meeting convened in midtown Manhattan. In attendance were the leadership of the SEC, the U.S. Department of the Treasury, and senior representatives of the NYSE, Nasdaq and securities firms. The subject was the reopening of the American capital markets.

While our first priority was to resume trading in a manner that would not hamper the heroic rescue work, there was also the question of the city's ability to resume public services and remove some of the debris. A related concern for the NYSE was whether the telecommunication infrastructure that the brokerage firms rely on to deliver orders and receive messages was available to manage the enormous amount of message traffic that would accompany a resumption of connectivity and trading. The decision to delay reopening the capital markets until Monday, September 17, 2001, also gave the telecommunications providers more time to reestablish connectivity among the various exchanges, marketplaces and firms that participate in trading equities. The goal was to ensure that the equity markets reopened in an orderly fashion with as many market participants as possible having reestablished their individual ability to trade.

Wall Street and the World Trade Center site are located in close physical proximity. Every trading day, thousands of employees arrive at the investment houses, banks and other financial intermediaries located in the financial district. Clearly, in the days following 9/11 it became increasing clear that the securities industry was in no position to resume business as

usual. Most importantly, we could not take the steps necessary to reopen if doing so could impede the rescue efforts underway at Ground Zero just blocks away.

The other issue that we faced was, in essence, a quality assurance problem. We wanted to ensure that we could resume equity trading in a manner consistent with the historical levels of deep liquidity and investor protection that are the hallmarks of the American capital markets. Stated otherwise, the test was whether we would be in a position to serve American investors with the same level of excellence that they and the world have come to expect of us.

An important part of our resilience is the flexibility and capacity of our technology, which was shown in our ability to host the entire American Stock Exchange (AMEX) equities trading floor in our Trading Floor on a few days notice after 9/11. The reconfigurable high-speed intranet technology that enables this is also the foundation of the capability that enabled us to create the contingency Trading floor within 90 days of 9/11.

During the six days following the September 11 attacks, the NYSE, in conjunction with SIAC, completed numerous tests necessary to ensure that the NYSE could reopen on Monday, September 17 and we assisted NYSE member firms in their preparations. We tested close to 1,000 NYSE member firm data communications lines into the NYSE's Common Message Switch system (CMS). We made more than 100 system, communication and database changes to permit NYSE member firms to reconnect with the Exchange's data centers. We worked with market data vendors to ensure the flow of real-time market data information to the NYSE's Trading Floor. On Friday, September 15 and Saturday, September 16, we conducted connectivity tests with NYSE member firms to ensure that they could deliver their orders to the NYSE's data centers. We prepared for the trading of American Stock Exchange equities at two posts on the NYSE's Trading Floor. In support of the National Market System (NMS) and the Options Price Reporting Authority (OPRA), we verified the connectivity for all participants and

vendors by providing continuous and extensive test time to all participating exchanges and recipients. Finally, the NYSE assisted several exchanges and vendors in reestablishing their connectivity to the NMS and OPRA systems.

The hard work and determination of thousands of individuals from September 11 through September 16 demonstrated to the world that the capital markets would not allow for the cowardly acts of terror perpetrated against the United States to initiate a systemic crisis in our capital markets. I am particularly proud of the tireless efforts of my partners at the NYSE who made certain that our trading platform was fully operational and able to handle then record volume of nearly 2.4 billion shares on Monday, September 17, 2001.

Critical Infrastructure

The NYSE has a long history of developing forward-looking business continuity strategies that "harden" or protect 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. Our IT infrastructure is connected to a private extranet that utilizes geographically redundant fiber routes. The NYSE and SIAC 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.

Contingency Planning

Contingency planning has also played a key role at the NYSE for many years. Pre-9/11, the NYSE and SIAC performed a comprehensive risk assessment to identify and address a wide array of man-made and natural threats to our critical systems, processes and infrastructure. Our plans included redundant, active data centers served by different power grids and multiple telecommunications facilities with each site sharing the processing load generated by the trading of about 1.5 billion shares daily. All of our facilities have back-up power generators and uninterruptible power source (UPS) systems. All of our facilities are interconnected through a diversely routed, auditable, private fiber optic network that does not pass through any telephone company central office.

Post 9/11 Business Continuity Initiatives

Since September 11, 2001, the NYSE has made an investment totaling more than $100 million, to prevent and/or recover from an interruption to our market. The specific business continuity programs include both new initiatives as well as significant enhancements to existing business continuity programs.

In particular, the NYSE has built a contingency Trading Floor, expanded SIAC's Emergency Command Center, created the Secure Financial Transaction Infrastructure (SFTI), constructed a remote network operations center and recently received approval to establish a remote National Market System (NMS) data center. The NYSE's Regulatory Group filed and the SEC approved new business continuity rules for NYSE Member Firms. In addition, to

ensure continuity of trading, the NYSE has also modified our system to accept four character symbols to back-up the Nasdaq.

In addition, we have enhanced NYSE and SIAC disaster recovery planning, physical security and information security, developed and implemented mandatory BCP training program for all NYSE and SIAC employees, enhanced emergency employee communications systems to ensure key personnel can be reached and all personnel have access to relevant and timely information in an event, instituted a temporal dispersion initiative with our data center staff. We are also adding generator capacity at the NYSE.

Operating the NYSE's data centers is a critical component of the NYSE's overall business continuity plan. All NYSE and SIAC departmental business continuity plans are continuously updated in light of 9/11 and the August 2003 blackout. We design, counsel and facilitate departmental and group business continuity planning (BCP) exercises. We have developed and implemented a mandatory BCP training program for all NYSE and SIAC employees. We have enhanced emergency employee communications systems to ensure that key personnel can be reached and all personnel have access to relevant and timely information in an event. SIAC has instituted a temporal dispersion initiative so that a significant number of its management and operational personnel are working off-site from the data centers at any time. In addition SIAC has added additional personnel to its Corporate Contingency Services team. SIAC has expanded and enhanced its Emergency Command Center with upgraded and new equipment. This same facility functions as the Emergency Command Center for the SIA during an event such as the August 2003 blackout. SIAC participates in the New York City Office of Emergency Management's Corporate Emergency Access Program. This program allows critical employees to gain access to the Manhattan sites in locations restricted to public access due to

emergency conditions - after the areas are deemed safe by local authorities for limited re-entry. As a result, critical operations can continue until "normal" conditions resume.

Physical Security Enhancements

The NYSE has strengthened its physical security in and around the primary Trading Floor at the Exchange's headquarters and at 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.

Immediately following 9/11, the New York City Police Department and the Mayor's Office created a security zone, which surrounds the NYSE. Seven intersections were closed to protect the NYSE and the financial district against the threat of a vehicle delivered explosive.

In partnership with the Lower Manhattan Development Corporation, New York City's Office of City Planning, the New York City Economic Development Corporation, the Alliance for Downtown New York, the New York Police and Fire Departments, Bank of New York and the New York Stock Exchange, the financial district's Streetscape and Security Plan is presently being implemented. This plan permanently secures each of those intersections as we beautify and make more pedestrian-friendly the Wall Street gateway to the financial district. NYSE Security Officers who have been sworn in as Special Patrolmen staff each of the seven intersections and they will work under the direction of NYPD Counter-Terrorism officers.

The Security Division continues to conduct daily threat assessments in cooperation with the U.S. Department of Homeland Security, the FBI, New York State's Office of Public Safety, New York City's Office of Emergency Management and the New York Police Department's Counter-Terrorism Bureau and Intelligence Division. Continuous evaluations of the NYSE's force protection and security procedures are conducted with special emphasis on delivery vehicles that enter the security zone. All incoming merchandise and mail are subject to canine explosive detection inspection as well as x-ray before they enter the zone and the NYSE.

Protection elements include outer checkpoints where we inspect carry-ins and the photo I.D. badges of employees; CCTV cameras are configured to digitally record all images within the perimeter; and proprietary armed security officers along with contract security officers in combination with an NYPD Hercules team provide force protection to our perimeter on a continuous basis. All persons who enter the NYSE are subject to security screening, which includes x-ray inspection of their carry-ins and a magnetometer screen of their person.

Security Division personnel continue to receive ongoing training in high-rise building safety, terrorism awareness, and counter-surveillance techniques as well as chemical, biological and radiological threat awareness.

At the NYSE's data centers, we have doubled the number of security personnel. Moreover, we have implemented new hiring standards requiring former law enforcement or military backgrounds for the security staff. We have enhanced training for SIAC security personnel, which includes counter-terrorism and physical force training. SIAC security personnel are armed and receive regular weapons training. We have established a 24-hour NYPD paid detail monitoring the perimeter of the data centers. There is a 24x7 canine bomb detection unit at each of our data centers. We have implemented traffic control and vehicle

screening at the checkpoints. We have installed fixed protective planters and movable vehicle barriers. We have created a new screening area with x-rays and magnetometers. There is an external perimeter screening post to check bags and packages. A New York City bus route was re-routed from a "drive through" located at one of the data centers. We acquired a parking garage at the data centers and only SIAC authorized employees may use this garage. Identification cards are required to gain entry and all vehicles are inspected at the garage entrance.

We have lowered SIAC's profile by removing SIAC's name from all entrances, maps, and area directories. We have installed x-ray units and magnetometers at the data center loading docks. A dock master supervises all deliveries. We have implemented digital closed circuit television coverage for the data center's interior, exterior and parking garages. Also, we have enhanced the security of SIAC's critical inter-site communications routes.

All employees, domestic and international, undergo comprehensive background checks - FBI, local criminal, Immigration and Customs Enforcement, Social Security Administration, residence, education and employment verification. All visitors that access SIAC facilities for at least three days during a two-week period undergo FBI, local criminal, residence, education and employment verification. All foreign companies doing business with SIAC are investigated. We have implemented electronic fingerprinting which has significantly reduced the turnaround time for criminal record checks.

The Contingency Trading Floor

In the weeks and months after the resumption of trading on September 17, 2001, the NYSE and SIAC continued its plan of risk mitigation and decided to develop and maintain a

contingency site. Approximately one year after September 11, 2001, the NYSE and SIAC outfitted and tested a contingency site. This alternative venue has the capability to support the trading of all NYSE-listed equity securities without modifications to the NYSE's market structure model and operate on a next-day basis should an event disable the primary Trading Floor. Support is provided for both specialists and brokers, and they have access to the NYSE's full suite of trading applications. The CTF can trade all securities processed at the Exchange today with the same technology used on the primary Trading Floor. A full range of logistical and support services are available at the contingency site. Equipment is checked daily, and quarterly simulations of the full trading day are performed at the contingency site to ensure smooth and reliable operation if necessary.

The Secure Financial Transactions Infrastructure ("SFTI")

The NYSE and SIAC have launched Secure Financial Transaction Infrastructure ("SFTI," pronounced "safety"), a private extranet to serve the financial industry. NYSE and SIAC designed and implemented the SFTI network, which combines recovery, redundancy, and diversity to provide continuous telecommunications resiliency and a secure means of connecting to trading, clearing and settlement, market data distribution, and other SIAC services to member financial firms.

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. In June 2004, Brian Roseboro, Undersecretary of the Treasury for Domestic Finance, joined the NYSE, AMEX, the SIA, the Bond Market Association and SIAC to praise this effort to enhance the resiliency of the financial system.

Instead of running circuits directly to SIAC, users 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 carries 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 making SFTI completely independent of all other telecommunications circuits and conduits. Therefore even if one SFTI fiber pathway is compromised, financial data traffic will continue to move uninterrupted along another pathway, improving the industry's protection against possible threats. Over 600 firms, including all of the major securities industry participants, are now connected to SFTI.

The Remote Network Operations Center

The NYSE and SIAC designed and built a remote network operating center ("RNOC"). The RNOC will allow for same-day recovery of technology and supporting infrastructure if the NYSE's data centers are inaccessible due to a regional event. We will have the ability to monitor and operate the data centers from the RNOC. The RNOC will support NYSE and National Market Systems (the Intermarket Trading System, the Consolidated Trade System, the

Consolidated Quotation System and the Options Price Reporting Authority) computer operations and the SFTI network. SIAC staff will operate the RNOC on a 24x7 basis and they will be able to assume the operations of all NYSE systems and the systems used to support the National Market System. The RNOC will be operating in the fourth quarter of 2004.

Remote National Market System Data Center

The Consolidated Tape Association/Consolidated Quotation Operating Committee (CTA/CQOC) directed SIAC to move one of the National Market System data centers away from the New York area. SIAC designed and is currently implementing a remote data center for them in support of the Consolidated Tape and Consolidated Quotation (CT/CQ) systems, and for the Options Price Reporting Authority ("OPRA") in support of the OPRA system. Taken together, the Consolidated Tape Association, which is comprised of the CT/CQ systems, the Intermarket Trading System ("ITS"), and the OPRA comprise the National Market System ("NMS"). The remote data center is scheduled to be completed and activated in the second quarter of 2005 and will operate at least one of the NMS systems at all times. Should the primary processing facility be unavailable, the remote data center will be able to run all of the OPRA, CT and CQ systems the following business day.

Unlisted Equities

The NYSE is ready to trade the top 250 Nasdaq stocks, which comprise almost 85 percent of Nasdaq's average daily volume. Each quarter we update the list of the top 250 stocks. The NYSE allocates, on a proportional basis to the NYSE's specialist firms, each of the top 250 Nasdaq stocks. This allocation file is saved for immediate activation.

NYSE-listed securities are identified by three or fewer character symbols, and our trading systems were previously configured to accept only up to three such symbols. All NYSE systems were modified and tested to accept and process four (or more) character symbols as of July 2001 used by such unlisted stocks. We currently have at least one five character stock symbol in the top 250 Nasdaq stocks. The NYSE tests the ability of our member firms to trade Nasdaq listed securities with the NYSE in the event Nasdaq is not operational. 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 will be adequate.

It should be noted that the NYSE has the capacity to process five times our current average daily volume of 1.5 billion shares. With the recent addition of capacity-on-demand from our technology vendors, our capacity is more than adequate to handle our current message traffic as well as the additional message traffic for the top 250 Nasdaq securities.

NYSE Rule 446

As a self-regulatory organization ("SRO"), the NYSE filed Rule 446 ("Business Continuity and Contingency Plans") on August 16, 2002 and the SEC approved it on April 7, 2004. NYSE Rule 446 mandates that NYSE member firms specifically define and continuously update business continuity plans. 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. Rule 446, which became effective August 5, 2004, also requires that a member's or member organization's business continuity plan (BCP) be reasonably designed to enable it to meet its existing obligations to customers, and address existing relationships with other broker-

dealers and counter-parties. Rule 446 also requires members and member organizations to conduct at least annually a review of their BCPs to determine whether modifications are necessary in light of changes to operations. However, BCPs must be updated whenever there is a material change in a firm's operations, structure, business, or location that affects the information set forth in the BCP.

Information Security

An ongoing component of the NYSE's contingency planning is a rigorous information security infrastructure. This infrastructure ensures the reliability of all information that we receive, process, and disseminate to the world every day. The NYSE utilizes a state of the art private network to process all order flow.

We employ external perimeters, intrusion detection, internal access controls, and we conduct penetration testing by using "friendly" hackers. A SIAC employee 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.

We have designed and implemented a full range of protections to ensure the confidentiality, availability and integrity of information transmitted to and from the NYSE and SIAC. Examples include firewalls and intrusion detection systems.

We have increased our focus on collective intelligence. Using various threat intelligence and analysis services, SIAC has increased its level of situational awareness regarding cyber threats and their potential impact on our networks and on the industry as a whole. SIAC participates in the ISAC program of information sharing, which allows the industry as a whole to gain a fuller picture of the nature and extent of threats and vulnerabilities.

We have increased internal and external network assessments to ensure that our systems operate with the highest possible level of security. All our critical networks are scanned for vulnerabilities daily and any issues found are dealt with expeditiously.

We have enhanced surveillance of the network traffic flowing between SIAC and the outside world. We have upgraded our Intrusion Detection Systems, allowing us to analyze IDS data for patterns of activity indicative of reconnaissance or attack.

SIAC has increased its monitoring of the Internet and other media for mentions of SIAC and our customers. We have taken a more proactive role in reviewing information to ensure that potential adversaries are not provided with information that could assist in attacks on the financial system of the United States.

We also regularly conduct reviews of publicly available information to determine what an adversary planning an attack would know about the NYSE and SIAC.

NYSE-SIAC Public-Private Partnerships

As an example, the NYSE and SIAC participate in or chair the following industry committee or task-forces which share information on business continuity preparation and preparedness, system security, disaster recovery and have taken leadership roles in the following public and private organizations:

- Securities Industry Association (SIA) Business Continuity Planning Steering Committee;
- Co-chair of the SIA Exchanges & Industry Utilities Committee;
- Co-chair of the SIA Industry Testing Committee;
- The President's National Security Telecommunications Advisory Committee (NSTAC);
- Financial Services Sector Coordination Council (FSSCC);

- Bond Market Association (BMA) Business Continuity Council;
- Chair of the Financial Services Information Sharing Advisory Council (FS/ISAC); and
- Chair of the ISAC Council, a coordinating body with representation from all the industry ISACs.

We also participate in the SEC Market Regulation Division's Automation Review Policy (ARP) reports and inspections, and we responded to requests from the GAO as part of their original study on financial markets initiatives following 9/11 – and their subsequent follow-up.

We have also 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 U.S. Department of Homeland Security or the SEC. The Exchange has established new 800 telephone 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.

The August 14-15, 2003 Blackout

The blackout of August14-15, 2003 was the first opportunity for the NYSE and SIAC to activate their contingency planning. A number of our business continuity initiatives were used during the fourteen hours that the NYSE and SIAC were without electricity from ConEdison. The overwhelming majority of the NYSE's management, technology, facilities and security personnel remained at the NYSE throughout the evening, as did SIAC's management and

operational staff. The SIAC Emergency Commend Center functioned as the Command Center for the Securities Industry Association during the blackout.

On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout. The blackout began shortly after 4:00 p.m. NYSE trading had closed for the day when the blackout began and the post-trade clearance and settlement processes were underway.

When the NYSE's data centers lost electricity, data center generators automatically started and no post-trade processes were affected. The NYSE did not start its generators until approximately 10:00 p.m. on Thursday, August 14. We hoped that the blackout was a temporary condition and we were in constant communication with ConEdison as well as New York City officials to determine when ConEdison could restore electrical power to the NYSE. When it became clear that ConEdison would not be able to restore electrical power until some time on Friday, August 15, the NYSE decided to start its own generators.

The NYSE's generators powered the NYSE's Trading Floor and the first six floors of the NYSE's headquarters until approximately 5:00 a.m. on Friday, August 15. ConEdison restored electrical power to the NYSE shortly after 5:00 a.m. and the NYSE opened at 9:30 a.m. on August 15. While trading was light, the NYSE did not experience any systemic problems.

The August 1 Heightened Terror Threat

On Sunday, August 1, 2004,Secretary Ridge of the U.S. Department of Homeland Security announced that al-Qaeda was targeting specific sites in Washington, D.C., Newark, New Jersey and New York City, including the NYSE. In addition, Secretary Ridge announced

that the Department of Homeland Security was raising the terror threat level to orange for New York City.

At approximately 6:00 p.m. on Saturday, July 31, the New York office of the FBI contacted NYSE security officials to inform them that the FBI had information that was very pertinent to the NYSE. The FBI requested that NYSE officials come to their New York offices immediately to review the specific intelligence obtained by the U.S. government. This intelligence clearly indicated that Al-Qaeda had surveilled the NYSE.

On Sunday, August 1, NYSE Security officials met with the FBI and NYPD Commissioner Ray Kelly. At this meeting, the FBI and the NYPD informed the NYSE that there would be an immediate increase of NYPD officers and NYPD Hercules teams deployed around the NYSE's perimeter. In addition, the NYPD would increase the number of truck inspections for vehicles traveling south of Canal Street to determine if those trucks actually needed to proceed downtown towards the financial district.

At 6:00 p.m. on Sunday, August 1, the NYPD called a meeting with security officials from broker-dealers located in and around Wall Street. At this meeting the NYPD pledged their assistance of NYPD assets and cooperation during the heightened alert.

Also on Sunday, August 1, the NYSE's CEO, John Thain, spoke with Secretary Ridge and New York City Mayor Michael Bloomberg to discuss the heightened threat level. The Department of Homeland Security as well as other Federal, state and local agencies notified the NYSE before the Secretary's announcement that the Exchange was a specific terrorist target. With this advance notice, the NYSE was able to communicate with its employees through our contingency websites. Using these contingency websites we were able to provide timely information about the status of our operations for Monday, August 2, to NYSE members,

member firms and member firm employees and NYSE employees. On Tuesday, August 3, NYSE officials met with Homeland Security Secretary Tom Ridge and New York City Mayor Michael Bloomberg where they both pledged their cooperation and provision of Federal and New York City assets as needed.

Since 9/11, all of our efforts have served to increase NYSE's physical security presence and its business continuity planning. Our enhanced business continuity and contingency planning are on-line and being tested every day. Unlike many localities and sites, New York City and the NYSE remain at a higher alert than the rest of the United States.

****

The NYSE is committed to ensuring that the U.S. capital markets remain the strongest and most resilient in 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 confidence to America's 85 million investors. While the NYSE and SIAC have implemented a comprehensive contingency plan that would provide for the orderly resumption of trading in the event of an attack or other catastrophe, we cannot prepare for every possible contingency. We will continue to work with the SEC, Department of the Treasury, the Department of Homeland Security, the NYSE's member firms, the financial services industry, and Federal, state and local law enforcement to address threats and to implement strategies and solutions.

I hope the foregoing is helpful to the Committee. 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.

STATEMENT

OF

WILTON DOLLOFF
EXECUTIVE VICE PRESIDENT
OPERATIONS AND TECHNOLOGY
HUNTINGTON BANCSHARES INCORPORATED

ON BEHALF OF
BITS AND THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

HOUSE FINANCIAL SERVICES COMMITTEE
UNITED STATES CONGRESS

HEARING ON
CRITICAL INFRASTRUCTURE PROTECTION

SEPTEMBER 8, 2004

TESTIMONY OF WILTON DOLLOFF
EXECUTIVE VICE PRESIDENT, OPERATIONS AND TECHNOLOGY
HUNTINGTON BANCSHARES INCORPORATED

Introduction

Thank you, Chairman Oxley and Ranking Member Frank, for the opportunity to testify before the House Financial Services Committee about the ways the financial services sector is addressing critical infrastructure protection.

I am Wilton Dolloff, executive vice president for operations and technology at Huntington Bancshares Incorporated. I am pleased to appear before you today on behalf of BITS and The Financial Services Roundtable (The Roundtable). Huntington is a $31 billion regional bank holding company headquartered in Columbus, Ohio. Huntington provides innovative retail and commercial financial products and services through more than 300 regional banking offices in Indiana, Kentucky, Michigan, Ohio and West Virginia. Huntington also offers retail and commercial financial services online, through its 24-hour telephone bank and through its network of nearly 700 ATMs. Financial services activities are also conducted in other states including Florida, Georgia, Tennessee, Pennsylvania, Maryland, New Jersey, and Arizona.

I am also a member of the Executive Committee of BITS, a nonprofit industry consortium of 100 of the largest financial institutions in the US. BITS is the sister organization to The Financial Services Roundtable. BITS members hold about $9 trillion of the nation's total managed financial assets of about $18 trillion. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. BITS is not a lobbying organization. Our work in crisis management coordination, cyber security, critical infrastructure protection and fraud reduction is shared not only among our member companies but throughout the financial services sector. We have set industry-wide technology standards and business requirements for enhancing security, managing vendors and reducing fraud, including best practices for preventing and reducing Internet fraud and managing service provider relationships. BITS works with other critical infrastructure sectors, government organizations including US Department of Homeland Security, US Department

of the Treasury, Office of the Comptroller of the Currency (OCC), the Federal Reserve, technology providers and third-party service providers to accomplish its goals.

We are fortunate to have excellent leadership within our sector. While BITS takes pride in its own role in enhancing the sector's preparedness, we recognize that collaboration and joint efforts with many of the other financial services industry associations can magnify the value of what we have contributed. One principal vehicle for this collaboration is the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), in which BITS participates. The FSSCC is chaired by the financial services sector coordinator, Don Donahue, Chief Operating Officer, Depository Trust and Clearing Corporation. The FSSCC fosters and facilitates financial services sector-wide activities and initiatives designed to improve critical infrastructure protection and homeland security, based on the close alliance and cooperation among BITS and the other FSSCC members to achieve these ends. BITS and other FSSCC members work closely with the Federal Banking Infrastructure Information Committee under the leadership of Wayne Abernathy, Assistant Secretary for Financial Institutions, US Department of the Treasury, and with the active participation of numerous government agencies responsible for the safety and soundness of the entire financial services sector.

Responding to the Challenge

Since 9/11, our sector has done a lot to respond to the risks we face today. Protecting our Nation's critical financial services infrastructure is a top priority. Senior financial services executives have dedicated countless hours to prepare for the worst and to deal with the associated challenges. These efforts have played a major role in helping financial institutions prepare for and respond to crises.

The financial services sector is a key part of the Nation's critical infrastructure. Ensuring that the payments system operates during times of crisis is essential to the Nation's wellbeing. Among industry sectors, the financial sector is particularly aware of the challenge, in part because customer trust is so vital to the stability of financial services and the strength of the Nation's economy. At the same time, our sector is a favorite target of cyber criminals as well as of terrorists, as was made clear on 9/11.

Protecting our Nation's critical financial services infrastructure is a top priority. Among other things, we have convened numerous conferences and meetings to bring together leaders and experts, developed emergency communication tools, strengthened our sectors' information sharing and analysis center (FS/ISAC), conducted worst case scenario exercises, engaged in partnerships with the

telecommunications sector and key software providers, compiled lessons learned from the 9/11 attacks and the August 2003 blackout, developed best practices and voluntary guidelines, and combated new forms of online fraud.

There are a variety of important elements of our strategy to protect the financial services sector and its critical infrastructure. These include improving communications during crises, enhancing the resiliency of telecommunications services and the energy sector, improving the security of software and cyber space, addressing new forms of online fraud, and improving oversight of third party providers—all of which in total is focused on assuring the safety, soundness, security and stability of the financial services critical infrastructure. I'd like to briefly highlight several efforts.

Improving Communications

A fundamental foundation of BITS' approach to critical infrastructure protection is effective communications. As one example, Crisis Management Coordination is one of BITS' highest priorities. BITS has opened participation in the Crisis Management Coordination Working Group to nonmembers, embracing public partners as well as representatives of member financial institutions. Among its key roles today is coordinating the industry during times of crisis through the BITS/FSR Crisis Communicator. This high-speed alert system rapidly notifies appropriate members of conference calls, during which industry leaders share information and make decisions. Most recently, BITS used the Crisis Communicator following the threat level escalation for the financial industry in certain regions on August 1. On that date, a Sunday, BITS held a conference call for members to ensure business continuity and the safety of personnel and physical assets. Senior executives from the nation's top 100 banks participated, including vice chairmen, CIOs, chief information security officers and chief technology officers. In addition, Assistant Treasury Secretary Abernathy participated in a call of the FSSCC to discuss the DHS announcement and the impact on the entire sector. In response to the August 1 announcement by DHS, financial services firms (beyond the four named institutions) took additional steps to increase physical security.

Many firms relied on the "considerations document" that BITS and the Securities Industry Association jointly developed in 2003 at the request of the FSSCC on behalf of the sector. This confidential document addresses security specifics for financial institutions to consider at each threat level of the Homeland Security Advisory System. This detailed series of suggested "threat level considerations" provides sector members with specific guidance on appropriate steps that individual organizations can implement to reduce vulnerabilities and provide additional protection for their employees. This guidance has played a key role in educating sector members about appropriate

measures in raising and lowering the intensity of their security precautions as appropriate at different threat levels. The financial services sector was the first to create such comprehensive guidelines, which have served as the basis for similar templates for other sectors.

The BITS Crisis Management Coordination Working Group has also helped member companies establish cross-industry crisis management procedures through the *BITS and FSR Crisis Management Process: Members' Manual of Procedures.* Additionally, members of this group share information and establish best practices to improve the industry's ability to prepare for and recover from large-scale business interruptions.

Strengthening the FS/ISAC

Our sector has continued to support enhancements to the Financial Services Information Sharing and Analysis Center (the FS/ISAC), which was initially launched in 1999, to help secure the financial services sector against cyber attacks. Membership in the FS/ISAC continues to grow, providing an important tool for members to share and analyze threat and vulnerability information. Recently, the FS/ISAC has agreed to serve as the repository for an anti-phishing data base, developed through the leadership of the BITS Fraud Reduction Program, and described in more detail below.

Enhancing the Resiliency of Telecommunications Services

One of the key "lessons learned" in recent years is our sector's dependence on other critical infrastructure sectors, namely telecommunications and power. As a part of our strategy to address reliability and resiliency issues, BITS approached the telecommunications industry in 2002 in an effort to identify and mitigate vulnerabilities and enhance recoverability. The cooperation between these two sectors has been unprecedented. BITS has worked with the National Communications System, Federal Reserve Board,, Federal Communications Commission, and telecommunications companies. Additionally, BITS CEO Catherine Allen sits on the board of the Network Reliability and Interoperability Council (NRIC), representing the interests of the financial services industry. The NRIC's mission is, in part, to assess telecommunications vulnerabilities and determine how to best address them.

Results of this collaboration include:

- A detailed and confidential assessment of interdependencies in a specific geographic area as a replicable model for other areas;
- Best practices in telecommunications and financial industry procurement practices and policies;

- Greater awareness of telecommunications industry priority access and recovery tools, such as the Government Emergency Telecommunications System (GETS) cards, Wireless Priority Service (WPS) and Telecommunications Service Priority (TSP) program;
- Pilots to model the costs of attaining greater diversity and redundancy in telecommunications services to the financial services industry;
- Completion of the NSTAC Financial Services Task Force Report on telecommunications resiliency issues;
- Adoption by BITS and Financial Services Roundtable CEOs of the Network Reliability and Interoperability Council (NRIC) best practices in physical and cyber security; and
- Education of both sectors on the importance of working closely together to identify and address issues.

The FSSCC, at its meeting next week, is expected to approve for widespread distribution throughout the financial sector a statement on telecommunications resiliency issues, intended to provide guidance to all financial firms—from the largest to the smallest—on how they can act to improve the resiliency of their own telecommunications infrastructure. This FSSCC statement will build further on the efforts undertaken by BITS and others I mentioned above.

Strengthening the Power Grid

BITS is also working with the electric power industry on interdependency issues. The August 2003 blackout in the Northeast provided an opportunity to test our assumptions about what would happen with a large scale loss of power. In general, the electric power industry performed well. Backup systems operated, alternate communications systems were used, and there was no measurable impact on settlements and payments. There was excellent cooperation and communications among the financial services regulators, Treasury and the private sector. And, despite the absence of landline telephones and waning cell phone batteries, the BITS and Financial Services Roundtable Crisis Management Coordination process functioned as it should—providing members with a real-time forum to exchange information.

In June 2004, BITS held the BITS Critical Infrastructure Forum, "Strengthening Resiliency of the Telecommunications and Energy Sectors." More than 100 executives from the financial services, telecommunications, energy, and chemical sectors attended. In addition, senior officials from Treasury, DHS and Federal Reserve Board participated. We discussed critical issues related to interdependencies among our sectors and developed an action agenda to address them.

Establishing Regional Coalitions

BITS was a key player in the outstanding success of ChicagoFIRST, a cross-sector coalition to address crisis and security issues within Chicago's financial community. In cooperation with the US Department of the Treasury, and the Boston Consulting Group, BITS today is writing a manual to help other coalitions apply that model in their regions. The purpose is to address region-specific needs for resilience, recoverability and continuity of financial services in a time of crisis. The FSSCC, again, plans to work to get this material broadly distributed throughout the sector to encourage these types of preparations.

Financial Industry Steps to Strengthen Cyber Security

Our industry has been working hard to strengthen cyber security. We have stepped up our efforts by sharing information, analyzing threats and urging the software and technology industry to do more to provide more secure products and services.

The state of cyber security is an alarming issue and critical to protecting the nation's infrastructure. As I speak, hackers are writing code to compromise systems. Viruses are epidemic. Hackers are closing the window between the discovery of a flaw and the release of a new virus. They are employing the tactics of spammers to rapidly spread their destructive code globally. We are increasingly concerned that a coordinated cyber attack of some kind could impact communications, Supervisory Control and Data Acquisition (SCADA) systems, or first responder systems and put all of us at terrible risk.

In October of last year, BITS increased its focus on flawed software with a Software Security and Patch Management initiative to respond to increasing security risks and headline-sweeping viruses. Our goal is to mitigate security risks to financial services consumers and the financial services infrastructure, ease the burden of patch management caused by vendor practices, and help member companies comply with regulatory requirements.

Also in October of 2003, BITS began forging partnerships with key software vendors most commonly used in our industry. In February of 2004, BITS and The Financial Services Roundtable held a Cyber Security CEO Summit. The event launched BITS and Roundtable efforts to promote CEO-to-CEO dialogue on software security issues. More than 80 executives from financial services, other critical infrastructure industries, software companies, and government discussed software vulnerabilities and identified solutions. A "toolkit" with software security business requirements,

sample procurement language, and talking points for discussing security issues with IT vendors was distributed to 400 BITS and Roundtable member company executives. One important deliverable from this Forum is the set of key Software Security Business Requirements, essential from the perspective of the financial services sector. These requirements and the full "toolkit" are available in the public area of the BITS web site, at www.bitsinfo.org.

A theme of the event was the importance of collaborating with other critical infrastructure industries and government. Since the Summit we have worked with all the associations representing the financial services industry, The Business Roundtable and some sector-specific associations.

In April 2004, BITS and The Financial Services Roundtable announced a joint policy statement calling on the software industry to improve the security of products and services it provides to financial services customers. The policy statement calls on software providers to accept responsibility for their role in supporting financial institutions and other critical infrastructure companies. BITS and the Roundtable support incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products. We are also seeking protection from US antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase. Additionally, as part of the policy, BITS and the Roundtable are encouraging regulatory agencies to explore supervisory tools to ensure critical third-party service providers and software vendors deliver safe and sound products and services to the financial services industry.

Today, we are working with software companies to create solutions acceptable to all parties. In June BITS announced it had successfully negotiated with Microsoft to provide additional support to BITS member companies for Windows NT. We have provided Microsoft and other software and hardware companies with the Software Security Business Requirements. BITS members agree that these requirements are critical to the soundness of systems used in the financial services industry.

This summer, BITS published best practices for patch management from the user's perspective. This document is available to the public at no cost and applicable to industries outside of financial services. It was created by BITS in response to the increasing urgency of patch implementation, given the speed with which viruses are targeting new vulnerabilities. Security issues aside, patch management and implementation alone can cost one financial institution millions of dollars annually. A BITS survey of member institutions, extrapolated to the financial services industry in total, yielded

this estimate—costs to the financial services industry associated with software security, including patch management, are approaching one billion dollars annually. The best practices help companies mitigate these costs.

In July, BITS published *The Kalculator: BITS Key Risk Measurement Tool for Information Security Operational Risks.* This tool helps financial institutions evaluate critical information security risks to their businesses. The tool starts with a list of common information security threats and vulnerabilities and matches them with corresponding controls to mitigate those risks. Using the tool, financial institutions score their own information security risks based on the likelihood of an incident, the degree to which the organization has defended itself against the threat, and an incident's possible impact. An institution can use the results to boost its ability to assess and mitigate risks to its information security program. The tool brings together an extensive body of information security risk categories outlined in international security standards and emerging operational risk regulatory requirements and combines them in one tool. Financial institutions can modify the tool to meet their unique needs.

BITS is participating in the Corporate Information Security Working Group (CISWG) which is sponsored by Congressman Adam Putnam, Chairman of the House of Representatives' Subcommittee on Technology, Information Policy, Intergovernmental Relations on the Census. CISWG is made up of corporate, industry and academic leaders and is working to pursue a private sector-driven approach to enhancing the protection of the nation's corporate computer networks. BITS is active in the best practices, incentives, and procurement subgroups. In addition, BITS has participated in task forces set up by DHS and several technology associations.

In October, BITS will hold an invitation-only Forum called "Protecting the Core." This event will allow executives from member companies, government, and invited vendors to come together to discuss how the significant risks and costs resulting from insecure devices, untrusted systems, and new threats/vulnerabilities impact core operations.

The Forum will focus on sharing best practices and identifying solutions, focusing on three critical areas: 1) creating strategies for evaluating internal and external risk; 2) deploying preventative measures in a dynamic environment; and 3) identifying incident-management best practices.

Finally, the BITS Product Certification Program is another important part of our work to address software security. The BITS Product Certification Program is a testing capability that provides

security criteria against which software can be tested. A number of software companies are considering testing. The criteria are also used by financial institutions in their procurement processes.

BITS is also working with other critical infrastructure industries and industry associations to help motivate a larger user movement. BITS' consultation and collaboration with The Business Roundtable resulted in that organization's widely publicized response to the state of software security. The Business Roundtable called on software producers and end users to work together to build a more unified defense against the increasing number and growing cost of cyber attacks.

Identity Theft and Phishing: Prevention and Victim Assistance

Just as financial institutions are a key target for hackers and other cyber criminals, our industry is increasingly the target of fraudsters operating online. BITS and The Financial Services Roundtable are responding to the escalation in identity theft with a series of steps to facilitate prevention of the crime and assist victims when it occurs. The goals of these efforts are to help maintain trust in the financial services system, assist member companies' customers, and mitigate fraud losses. BITS and The Roundtable are working with the Administration, Congress, and law enforcement and regulatory agencies to accomplish these goals.

A cornerstone to these efforts is the BITS/FSR Identity Theft Assistance Center. Developed by BITS and the Roundtable, with the support of 50 founding member institutions, the ITAC is in pilot at this time. The concept is to provide a simplified recovery process that benefits victims by relieving much of the current burden of reporting the theft and restoring one's financial identity. Once an individual has reported a theft to his or her financial institution, and the problem has been solved at that institution, with the victim's permission, the ITAC will work with the consumer to determine whether accounts at any other institutions have been affected. If so, the ITAC will step in to notify all other companies where there may be an affected account. By working with the Federal Trade Commission and law enforcement agencies, information collected by the ITAC will be used to prevent future identity theft crimes. .

Because a consistent understanding of the problem is essential to finding solutions, a 2003 BITS white paper on identity theft outlines the full identity theft landscape, establishing key terms as well as identifying factors that contribute to identity theft. Background about the legislative and policy environment, including existing and proposed laws, is provided as well as industry best practices.

Along with the white paper, BITS developed guidelines for financial institutions to use to prevent identity theft and restore a victims' financial identity. Included are processes for providing a "single point of contact" at companies to whom victims may report cases of identity theft.

Additionally, the BITS Fraud Reduction Steering Committee and the Federal Trade Commission have created a Uniform Affidavit to simplify the recovery process for victims. The Uniform Affidavit streamlines the reporting process by recording the victim's information about the crime, so that victims only have to tell their story once

BITS is also responding to "phishing" through its Fraud Reduction Program. Phishing is the practice of luring consumers to provide bank account and other personal information to fraudsters through bogus email messages. In response to these and other online scams, BITS is creating a Phishing Prevention and Investigation Network. The Phishing Network will provide member institutions with information and resources to expedite investigations and address phishing/spoofing incidents. The Phishing Network will include a searchable database of information from other financial institutions on their phishing incident and response experience, including contacts at law enforcement agencies, foreign governmental agencies, and ISP Web administrators. The Network will also provide data on trends to help law enforcement build cases and shut down identity theft operations.

The BITS Phishing Prevention and Investigation Network will:

- Help member institutions monitor and shut down e-scams faster and more effectively.
- Reduce financial institution manpower costs and losses.
- Increase phishing investigations and arrests of perpetrators.
- Facilitate communication among fraud specialists at financial institutions, service providers and law enforcement agencies.

Complying with Regulatory Requirements

As you know, financial institutions are heavily regulated and actively supervised by the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of Currency, Office of Thrift Supervision, National Credit Union Administration, and the Securities and Exchange Commission. Regulators have stepped up their oversight on business continuity, information security, third party service providers, and critical infrastructure protection. Our industry is working consistently and diligently to comply with new regulations and ongoing examinations. In addition, organizations like BITS and other industry associations have developed and disseminated voluntary

guidelines and best practices as part of a coordinated effort to strengthen all critical players in the sector. Regardless of how well institutions respond to regulations, we simply cannot address these problems alone. Our partners in other critical industry sectors—particularly the telecommunications and software industries—must also do their fair share to ensure the soundness of our nation's critical infrastructure.

Lessons Learned

BITS regularly gathers and disseminates "lessons learned" from its membership. These lessons are a critical building block for BITS' best practices. Below are some of those lessons for the Committee to consider.

We must work with other parties in the private and public sectors to address these issues sufficiently. We understand that the risks for national security and economic soundness cannot be underestimated. Neither can the importance of our working together to address them.

We need to look strategically and holistically at the nation's critical infrastructures and what can be done to enhance resiliency and reliability. We urge the Committee to consider all aspects of critical infrastructure—the software and operating systems, the critical infrastructure industries, and the practices of firms, industries and the government—in addressing software security and vulnerability management.

Preparation is critical. The events of 9/11 and subsequent preparations by the private sector and government enhanced mutual trust and the ability to communicate, shift to backup systems, and continue operations. Prior to the August 2003 blackout, BITS had conducted a scenario exercise that included the West Coast power grid being out for seven days and the impact that might have on the sector. That exercise helped the industry think through things like communications, water shortages, backup for ATM operations, and fuel for generators.

Critical infrastructure industries and the public need to have an early understanding of the scope and cause as early as possible when a major event occurs. During the August 2003 blackout, the announcement that the problem was not the result of a terrorist event alleviated public concerns and made for orderly execution of business continuity processes. If it had been a terrorist event, other communications and directives such as "shields up"—in which external communications to institutions are blocked—might have occurred.

Diverse and resilient communication channels are essential. Diverse elements—such as cell phones, wireless email devices, landline phones, and the Internet—are required. Both diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services will be maintained.

The power grid must be considered among the most vital of critical infrastructures and needs investment to make sure it works across the nation. The cascading impact on the operation of financial services, access to fuel, availability of water, and sources of power for telephone services and Internet communications cannot be overstated.

Recognize the dependence of all critical infrastructures on software operating systems and the Internet. A clear understanding of the role of software operating systems and their "higher duty of care," particularly when serving the Nation's critical infrastructures, needs to be explored. Further, the Committee should recognize that the financial sector is driven by its "trusted" reputation as well as regulatory requirements. Other industries do not have the same level of regulatory oversight, liability, or business incentives. However, we rely on other sectors because of our interdependencies. Responsibility and liability need to be shared.

Recommendations

The Congress can help the financial services sector meet the challenges of a post 9/11 environment in a number of ways. We have developed these key recommendations for the Committee to consider:

1. **Recognize that the financial sector is driven by its "trusted" reputation as well as regulatory requirements. Other industries do not have the same level of regulatory oversight, liability, or business incentives.** However, we rely on other sectors because of our interdependencies. Responsibility and liability need to be shared.

2. **Maintain rapid and reliable communication.** Critical infrastructure industries and the public need to have an early understanding of the scope and cause as early as possible when a major event occurs. During the August 2003 blackout, the announcement that the problem was not the result of a terrorist event alleviated public concerns and made for orderly execution of business continuity processes. Diverse communication channels such as cell phones, wireless email devices, landline phones, and the Internet are necessary. Both

diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services will be maintained.

3. **Recognize the dependence of all critical infrastructures on software operating systems and the Internet. Given this dependence, the Congress should encourage providers of software to the financial services industry to accept responsibility for the role their products and services play in supporting the nation's critical infrastructure.** In so doing, Congress should support measures that make producers of software more accountable for the quality of their products and provide incentives such as tax incentives, cyber-insurance, liability/safe harbor/tort reform, and certification programs that encourage implementation of more secure software. Congress also could provide protection from US antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase.

4. **Encourage regulatory agencies to review software vendors—similar to what the regulators currently do in examining third-party service providers—so that software vendors deliver safe and sound products to the financial services industry.**

5. **Encourage collaboration and coordination among other critical infrastructure sectors and government agencies to enhance the diversity and resiliency of the telecommunications infrastructure.** For example, the government should ensure that critical telecom circuits are adequately protected and that redundancy and diversity in the telecommunications networks assured.

6. **Invest in the power grid because of its critical and cascading impact on other industries and other critical infrastructures.** The power grid must be considered among the most vital of critical infrastructures and needs investment to make sure it works across the nation.

7. **Establish improved coordination procedures across all critical infrastructures and with federal, state, and local government when events occur.** Coordination in planning and response between the private sector and public emergency management is inadequate and/or inconsistent. For example, a virtual national command center for the private sector that links to the Homeland Security Operations Center would help to provide consistency.

8. **Encourage law enforcement to prosecute cyber criminals and identity thieves, and publicize U.S. government efforts to do so.** These efforts help to reassure the public and businesses that the Internet is a safe place and electronic commerce is an important part of the Nation's economy.

Protecting critical infrastructure is a collaborative and cooperative effort. Only by working together can we address the challenges we face today. On behalf of Huntington Bancshares, BITS, and The Financial Services Roundtable, thank you for the opportunity to testify before you today.

Samuel H. Gaer, Chief Information Officer
Of the New York Mercantile Exchange

Before the United States House of Representatives
Committee on Financial Services

Hearing Entitled
"Protecting our Financial Infrastructure: Preparation and Vigilance"

September 8, 2004

Good Morning. Thank you, Chairman Oxley and members of the committee for inviting me to address the issue of emergency preparation and vigilance for the financial services sector. The subject matter is of timely concern and I sincerely welcome the opportunity to both express what the New York Mercantile Exchange (the Exchange) has accomplished to date, as well as to express concerns regarding areas in which you might consider providing assistance to our efforts going forward.

The Exchange is the world's largest physical commodity futures exchange and has been an example of market integrity and price transparency throughout its 132-year history. Commercial enterprises and government entities all over the world use our futures and options contracts to manage their energy and metals risk, a function that is particularly critical to the global economy in any time of crisis – whether it be a natural or man-made disaster.

The Exchange also plays a vital role in the commercial, civic, and cultural life of New York. It provides thousands of jobs in the financial services and allied industries, and through the

Exchange's Charitable Foundation supports cultural and social service programs in the NYC downtown community, throughout the tri-state area where our traders and staff live, Washington, D.C., Houston, TX, and across the country.

The Exchange also endeavors to be a technology leader in the futures industry by providing first-class end-customer software and services as well as developing robust, redundant, and best-of-breed trade management, clearing, and reporting systems capable of quick failover to backup systems when required.

I would like to cover our accomplishments on this subject and provide this committee with the status of our current readiness; what improvements we are planning, the experiences and lessons from 9/11, the blackout of 2003, our testing, our planning for the events and possibilities surrounding the Republican National Convention (RNC), and finally, areas that this committee might consider to aid the ability of this sector to recover during a future emergency.

The Exchange's emergency preparedness efforts may be broken into several distinct but integrated categories: a) the holistic discipline of business continuity planning, b) the more traditional and more narrowly-focused practice of disaster recovery planning, c) the education of the critical staff responsible for our emergency preparedness, and finally, d) the Exchange's external efforts, including coordinated industry testing and providing valuable feedback to the concerns of government and industry agencies and committees such as yours.

No preparedness planning can be accomplished without a careful analysis of the business being protected. It is of critical importance to understand what processes make up our business. Once these are identified they must be prioritized, and this can only be accomplished by assessing the risks and possible impact of those risks on our business through conducting a risk and impact analysis. The Exchange's business continuity planning is based on both of these reviews.

Our core business is trading and clearing. In order to ensure the continuity of this core business, we have pursued several alternatives. The Exchange headquarters was designed to be as redundant as possible including the availability of a back-up generator, which became critical during the blackout of 2003. One of the first priorities for the Exchange after September 11 was to build a replica trading floor. This floor, which was completed in January 2003, is located outside the city, but still within the metropolitan area. It contains full operational trading rings, telephone workstations and booths, and administrative space, as well as a live price feed to the outside world. It would be no more than a couple of hours commute for the furthest trader or staff member. All of our traders and key employees have been provided with directions to the site and, in the spring of 2003, many of our traders participated in a mock trading simulation at the site.

In a situation where access to either site was not immediately available, the Exchange also has two electronic trading systems, both of which have 'round the clock trading capability. In fact, we were the first exchange in New York to reopen following September 11, when we reopened our electronic trading system for a two-hour session on September 14. In those two hours, a record of more than 70,000 contracts were traded electronically as firms leapt for access to the critical energy and metals markets that hadn't been available to them for three days.

The Exchange's business is also comprised of many different process groupings, each of which requires a particular expertise. These business units are each assigned a staff person as well as a backup – called business continuity coordinators (BCCs) - whose responsibility it is to assess the critical processes and to create a workable plan to recover these processes, prioritized according to the risk and impact analysis. The BCC is an individual with working experience and knowledge of the procedures in their specific business unit. The role of continuity coordinator is in addition to their primary job functions. The Emergency Operations Team (EOT), which I will

describe in a few moments, is comprised of the continuity coordinators and the Business Continuity Leader (BCL), whose role it is to coordinate the Exchange's continuity and disaster recovery efforts, head the EOT, and report to the Crisis Management Team.

During an emergency the high-level, strategic decision making authority rests with the Crisis Management Team (CMT). The CMT comprises the five executive committee members of the board of directors, chief officers, and other critical senior executives. Their role is to assess a threat and, if necessary, provide an official declaration of a disaster; to interface with the members of the Exchange; and to coordinate with industry and regulatory agencies. They have been empowered by the board of directors to make the critical business decisions necessary in any emergency recovery effort.

Tactical decisions rest with the EOT; this is where the "rubber meets the road." As described above, the EOT is composed of the BCCs, each of whom is responsible for deploying one of the plan modules. These modules are separate, but coordinated plans, and may be deployed all at once, or separately as the emergency requires.

During any emergency, there is a requirement for a safe and secure place for emergency teams to assemble and manage recovery efforts and coordinate resources. The Exchange maintains emergency operations centers (EOC) at the primary and backup sites. The EOC is a secure area where the CMT can go to manage any event it may face. Each location is prepared with whiteboards, copies of the plans, computers, and digital and analog phone service.

Maintaining communication between recovery units and resources is the single most important aspect of any emergency recovery effort. All aspects of our emergency operations are choreographed via multiple communications links between resources and the Exchange's responders, and are coordinated and managed using an array of communications tools. The Exchange provides multiple layers of tools, which the team members use in the event one or more

fails. Each critical CMT member has been issued a cell phone with a two-way radio, a portable two-way email device - some of which can be used to make emergency phone calls -, a laptop, remote connection software to send and receive data to our network, and a cellular modem card to wirelessly connect to Exchange system resources from anywhere cellular coverage is available. Also available are multiple team-specific conference call numbers, which enable the team to conduct virtual meetings; websites to communicate information to customers, staff, and members; and toll-free hotlines to receive and provide critical information. In addition, the CFTC has sponsored the Exchange to take advantage of the National Communications System's Government Emergency Telecommunications Service (GETS). All critical team members have been issued this important tool.

Disaster recovery planning specifically refers to restoring the information technologies that run our business and provide services to staff and customers. Every critical Exchange system is duplicated and can provide services in the event the main facility or system is unavailable. Data moves across redundant optical fiber links, linking our backup site to the primary site, and allows synchronous or asynchronous replication of data, in both directions. In addition to the wide-area network created between the two hot-sites, the Exchange maintains multiple links to internet service providers.

Training, education, and regular testing will ensure that the systems and staff are ready to respond to any event that disrupts our business. Ongoing planning for events such as approaching hurricanes, planned transit strikes, or the RNC keeps the Exchange's planners in top form. The EOT meets regularly via the pre-configured conference bridge to discuss continuity planning, updating plans, and changes in business processes.

Our industry relies on a complicated inter-relationship of many companies and services. The Exchange is among the leaders in an industry-wide initiative to standardize the protocols

governing the way companies send and receive data. This will allow many companies to develop systems based on a standardized set of protocols, making it easier to deploy and maintain data communications under difficult circumstances. The Exchange and the Futures Industry Association (FIA) have begun planning a major multi-company and multi-exchange coordinated testing effort, which will culminate in a first annual industry-wide disaster recovery test this fall on Saturday, October 9th, 2004. The Exchange already does its own limited testing with member firms. However, this planned test will involve multiple exchanges as well as recovery service providers and independent software vendors. The effort is extremely important to our industry and will be repeated annually.

As a critical infrastructure organization we strive to learn from every event we face. So what were the lessons learned from 9/11, the 2003 Blackout, our mock disaster testing, and planning for the RNC?

The tragic and cataclysmic events that took place on September 11, 2001 showed us that planning for emergencies that involve a single company, building, or service is no longer adequate. Continuity planners must envision and plan for emergencies affecting multiple companies, buildings, infrastructure services, and utilities – emergencies that disable telecommunications, utilities, transportation, vendors, and customers. Multiple layers of communications options must be available to the emergency responders as well as the ability to manage a recovery effort on the fly with mobile technologies that allow the responders to collect information and direct resources. This testimony is a high-level glimpse into the thoroughness of the thought and action we have strived to apply to our recovery planning.

As we look back at 9/11, the relationships the Exchange has forged with government agencies will always be of critical importance, in planning for -- and support during -- an emergency event. The relationships our member firms have formed with important government leaders have

enabled the Exchange to overcome many difficult recovery challenges in the past. Necessary assistance was provided with water transportation for critical Exchange staff, as well as creating access through frozen zones for traders and staff, trucks carrying food, and also fuel deliveries for the Exchange's backup generators.

The blackout of 2003 taught us different lessons. The foremost of which is that a direct hit to a facility is not required to impair our ability to operate. Multiple redundant service providers need to be secured for all critical business services. This event also taught us that as good as our recovery plans are, they are only as good as the customers and business partners we rely on. Part of our vigilance must be to make sure our banking, clearing, and broker partners have themselves planned and prepared.

Other events that Exchange planners carefully considered - the approaching hurricane Isabel in late summer 2003, the planning we have done for the Republican National Convention, and the regular disaster recovery testing and mock disasters that the Exchange conducts all serve to reinforce and fine-tune the planning we have at-the-ready.

Communication stands alone as the key equalizer when facing the surprises any emergency delivers. No plan can forecast the effects generated from a disaster but having good communication plans in place allows our organization to counter this problem with the ability to change course as the emergency response requires – and to immediately communicate those course changes to traders, brokerage firms, clearing firms, customers, and staff.

Chairman, in closing, I ask that this committee consider the following concerns from the Exchange.

As an integral part of the critical infrastructure, the Exchange already manages a full compliment of continuity plans, backup sites, and emergency operations locations. Uninterruptible power supply systems, backup generators, and redundant data and voice

providers protect our facilities. However, our business necessarily relies upon the coordination of many services within the financial sector. It also relies heavily on the telecommunications, utility, and transportation infrastructure supporting that complex matrix of business partners, over which the Exchange has no control. The Exchange is prepared to recover our systems and business processes if faced with another event such as 9/11. But, the recovery of the services and the price discovery mechanisms we provide to the financial services sector and economy also relies on the resiliency of the external businesses on which the Exchange depends.

I would like to thank the Chairman and the members of this committee for inviting the Exchange to speak with the other distinguished panelists on this extremely important topic. I would be happy to answer any questions the committee has.

Statement by
Robert Liscouski
Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security
Before the House Financial Services Committee
September 8, 2004

Good morning Chairman Oxley, Congressman Frank and distinguished members of the Committee. I am pleased to appear before you today to discuss the protection of the financial services sector, including some of the more specific actions the Department of Homeland Security (DHS) has taken after the recent elevation of the threat level to Code Orange for the financial services sector in New York City, Northern New Jersey, and Washington, DC.

Established by the Homeland Security Act of 2002, IAIP leads the Nation's efforts to protect our critical infrastructure from attack or disruption. The IAIP Directorate was created to analyze and integrate terrorist threat information, and to map those threats against vulnerabilities -- both physical and cyber -- to protect our critical infrastructure and key assets.

IAIP includes the Homeland Security Operations Center (HSOC), the Office of Information Analysis, the primary analytic center for threat information and intelligence within DHS, and my office, the Office of Infrastructure Protection (IP). IP's mission is to lead the coordination of Federal, State, and local efforts to secure the Nation's infrastructure.

Recognizing the potentially devastating effects of disruption of services or catastrophic failures in the banking and financial sector, IAIP works on a daily basis to assess threats and vulnerabilities; mitigate risk; develop protective measures; and communicate with the sector. The banking and finance sector not only represents both physical and cyber vulnerabilities, but it is also critically interconnected with every other critical sector within our Nation.

IAIP Coordination and Information Sharing

As directed by Homeland Security Presidential Directive 7, IAIP has focused on monitoring and assessing threats and vulnerabilities to all sectors, including the banking and finance sector. Sharing this information with the private sector and other government entities is a vital component of IAIP's mission.

In preparation for responding to threats and elevated threat levels, IAIP has been building and coordinating a two-way exchange of information with the public and private sectors. These efforts have also included building relationships with the private sector and government entities as well as implementing and integrating technical and information sharing solutions.

The Homeland Security Information Network (HSIN) - Critical Infrastructure (CI) was launched earlier this summer and was specially designed to communicate real-time information to owners and operators of critical infrastructure, 85 percent of which is owned by the private sector. HSIN–CI has the capacity to send alerts and notifications to the private sector at a rate of:

- 10,000 simultaneous outbound voice calls per minute
- 30,000 inbound simultaneous calls (hot line scenario)
- 3,000 outbound simultaneous faxes
- 5,000 outbound simultaneous Internet e-mail

In addition, the Homeland Security Operations Center (HSOC) regularly disseminates terrorism-related information generated by IAIP, known as "products," to Federal, State, and local governments, as well as private-sector organizations and international partners. The HSOC communicates in real-time to its partners by utilizing HSIN internet-based counterterrorism communications tool, supplying information to all 50 states, Washington, D.C., and more than 50 major urban areas. Threat products come in two forms:

- Homeland Security Threat Advisories, which are the result of information analysis and contain actionable information about an incident involving, or a threat targeting, critical national networks, infrastructures, or key assets. They often relay newly developed procedures that, when implemented, significantly improve security and protection. Advisories also often suggest a change in readiness posture, protective actions, or response.

- Homeland Security Information Bulletins, which are infrastructure protection products that communicate information of interest to the Nation's critical infrastructures that do not meet the timeliness, specificity, or significance thresholds of Threat Advisories. Such information may include statistical reports, periodic summaries, incident response or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools.

Sector Coordinating Councils and Sector Information Sharing

The Financial Services Sector has developed two effective mechanisms for the two-way sharing of information. The first is the Financial Services Sector Coordinating Council (FSSCC), which consists of senior representatives of major financial institutions representing a cross section of the financial industry. The FSSCC provides an orderly and effective venue for the financial sector and the Government to engage on the broad range of Homeland Security and critical infrastructure issues. In addition, the financial sector maintains the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC was established in 1999 under the aegis of a Financial Services Steering Committee (now the Financial Services Sector Coordinating Council) representing the sector. It provides a mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information to and from its members and the

Federal Government. Every two weeks the FS-ISAC conducts threat intelligence conference calls at the unclassified level for subscribed members, with IAIP providing input. These calls cover physical and cyber threats, vulnerabilities, incidents that have occurred during the previous two weeks, and suggestions and guidance on future courses of action.

Sector Coordinating Councils are emerging as a primary conduit for communication and coordination with the Federal government and many critical infrastructures and key resource industries. Private industry, on its own volition, organizes these forums to address national planning, common issues, develop best practices, and to find common solutions. Most sectors have established information sharing entities, such as Information Sharing and Analysis Centers (ISACs) to collect information on cyber and physical incidents and to disseminate alerts, warnings, and advisories to their members. At times, they also provide the communication vehicle for best practices and other security information tailored for each sector.

The Sector Coordinating Councils and their ISACs maintain and provide DHS with distribution lists which allow them to quickly disseminate threat warnings, alerts and advisories to members of their sectors. Information provided by the sectors is incorporated into the DHS situational awareness picture together with Intelligence Community and Law Enforcement information concerning possible threats to the nation's critical infrastructures. In addition, DHS has established close working relationships with the appropriately cleared senior sector members, including members from the financial services sector, to exchange classified information as appropriate.

IAIP receives and evaluates current threat and incident information, including suspicious activity reports, submitted directly by the industry or through their information sharing entity, and provides timely feedback on those issues. As recent events have demonstrated, during times of elevated threat, IAIP intensifies its efforts to coordinate and reach out to the private sector, the entities described above and other government agencies.

Protection of Critical Infrastructure

Terrorists are willing to exploit a wide range of infrastructure vulnerabilities. That is why we must continue to be vigilant and flexible in our approach to infrastructure protection.

Since the signing of Homeland Security Presidential Directive-7 in December 2003, IAIP has been engaged in numerous activities to protect our Nation's critical infrastructure, including the development the National Infrastructure Protection Plan (NIPP), a key requirement of the Directive. The NIPP will delineate roles and responsibilities among the federal, state, local, and private sector stakeholders, establish national goals for critical infrastructure protection, and describe how DHS will lead the effort to integrate critical infrastructure protection activities across the sectors.

As a key part of the NIPP, the Sector-Specific Agencies designated in HSPD-7 are developing plans to identify critical infrastructure assets; identify and assess vulnerabilities and prioritize sector assets; develop protective programs; and measure the effectiveness of these programs. IAIP has worked closely with the Department of Treasury to develop the Banking and Finance sector plan.

In today's highly technical and digital world, we recognize that attacks against us may manifest themselves in many forms, including both physical and cyber attacks. In addition, we recognize the potential impacts one attack may have on a variety of other assets. This interconnected and interdependent nature of our infrastructure makes our physical and cyber assets difficult to separate, and it would be irresponsible to address them in isolation.

IAIP is working closely with the Science and Technology Directorate, other entities across the Department of Homeland Security, the Departments of Defense and Commerce, as well as the private sector to develop better methods for assessing the trustworthiness of cyber systems and the software which drives the financial services and other critical infrastructures of our nation. Software produced both domestically and offshore may have unintended flaws. Efforts are underway to work with the private sector to ascribe better measures of trustworthiness to software products and focus on achieving a number of common objectives. Such objectives include lowering development costs, reducing the time required to assess systems, and enhancing security protocols.

In addition, the Department of Homeland Security unveiled the National Cyber Alert System, an operational system developed to deliver targeted, timely, and actionable information to Americans to secure their computer systems. It is important to inform the public about the true nature of a given incident, what the facts are, and what steps they can and should take to address the problem. The National Cyber Alert System provides that kind of information. We have already issued several alerts and products in a periodic series of "best practices" and "how-to" guidance messages. We strive to make sure the information provided is understandable to all computer users, technical and non-technical, which reflects the broad usage of the Internet in today's society.

Working with IP, the United States Secret Service joined forces with the Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center (CERT/CC), in order to conduct the Insider Threat Study. The study is a collaborative effort to better understand insider activities affecting information systems and data in critical infrastructure sectors, to include the banking and finance sector. This study is the first of its kind, and provides a comprehensive analysis of insider actions by analyzing both the behavioral and technical aspects of the activity.

The Insider Threat Study examines incidents when employees intentionally exceeded or misused an authorized level of system access that affected the organization's data, daily business operations, system security, or other areas via a computer. The study focuses on the on-line behaviors and communications that insiders engaged in before the incidents.

The goal of the study is to determine whether information may have been known or detectable prior to the incident; and to develop information to help private industry, government, and law enforcement better understand, detect, and ultimately prevent harmful insider activity.

On August 24, 2004, the first part of the report was released to the public sector; it is referred to as the Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. This portion of the report focused on individuals who have had access to and have perpetrated harm using information systems in the banking and finance sector, which includes credit unions, banks, investment firms, credit bureaus, and financial institutions. The findings highlighted in this area of the report are of great benefit to the financial sector, as it provides concrete examples of how insiders accomplished their activities and offers suggestions on what security and/or policy procedures may have deterred or prevented such activity from occurring.

IAIP Response to Recent Intelligence Involving the Financial Services Sector

The IAIP response in the financial sector was spurred by concerns over al-Qaida's interest in targeting U.S. critical infrastructure as well as recent intelligence revealing detailed reconnaissance against several U.S. financial institutions. Based on the multiple reporting streams and the information contained in these reports, the Intelligence Community concluded that the information warranted the heightened alert status.

The level and specificity of information found was alarming, prompting DHS raise the threat level to ORANGE for the financial services sector in New York, northern New Jersey and Washington, D.C. on Sunday, August 1. This was the first time the level had been changed for an individual sector and geographic-specific area.

In response to the heightened threat level, IAIP acted on several fronts to address the threat. In accordance with established DHS notification protocol for raising the threat level, conference calls were arranged between DHS, FS-ISAC, FSSCC, FBIIC, State homeland security personnel, and local law enforcement officials or entities. The Financial Services Roundtable, a private sector group representing the electronic commerce interests of the largest bank holding companies in the United States, was also included along with numerous other financial sector entities. In addition, senior leadership personally met with CEOs and Security Directors from the financial sector to better inform them of the evolving conditions and to provide guidance.

Simultaneously, Secretary Ridge activated the Interagency Incident Management Group (IIMG) to monitor and assess threat conditions. The IIMG is a headquarters-level multi-agency coordination entity that facilitates Federal domestic incident management activities. The mission of the IIMG is to provide strategic situational awareness, synthesize key intelligence and operational information, frame operational courses of action/policy recommendations, anticipate evolving requirements, and provide decision support to the Secretary of Homeland Security and other senior officials as requested during select periods of heightened alert and national-level domestic incidents. To

accomplish this mission, the IIMG is task-organized to include representation from DHS components and staff offices as well as a tailored group of interagency participants.

Subsequent to providing immediate alerts to the financial sector regarding the threat, IAIP continued to work with the industry to ensure that all targeted financial institutions were individually briefed. I AIP coordinated with Federal, State, and local law enforcement entities to ensure that the appropriate information was exchanged between the government and the private sector. IAIP also polled the various financial institutions to determine what additional protective measures were implemented as a result of the heightened alert. This included the deployment of IAIP personnel to provide technical assistance to local law enforcement and facility owners and operators.

IAIP personnel were also immediately deployed to facilities in Washington, DC, New York City, and northern New Jersey. Teams of IAIP personnel conducted Site Assistance Visits (SAVs), in collaboration with local law enforcement officials and asset owners and operators, to facilitate vulnerability identification and discuss protective measure options. A total of 21 visits have been conducted thus far of facilities in the banking finance sector. Owners, operators, and security personnel were also given Common Characteristics and Vulnerability (CCV) reports and Potential Indicators for Terrorist Attack (PITA) reports to help them identify vulnerabilities and precursors to terrorist attacks.

In addition to SAVs, IAIP personnel have been working with individual facilities and local law enforcement entities to implement buffer zones around select banking and finance facilities. Buffer zones are community-based efforts focused on rapidly reducing vulnerabilities "outside the fence" of select critical infrastructure and key resources. To support these efforts, IAIP provides assistance to local law enforcement officials to develop and implement buffer zones. To date, six buffer zone implementation plans for the banking and finance sector have been submitted to IAIP by State homeland security advisors.

Information gathered from SAVs and buffer zone implementation plans, and updates from the threat data, was given to the Principal Federal Official (PFO) in New York City. IAIP personnel were assigned to the PFO staff to provide expert, subject-based knowledge and act as a conduit to resources held by the rest of the department. IAIP supported the New York PFO in the days leading up to and during the Republican National Convention with updated information, technical expertise, and material assistance when appropriate.

At this time, IAIP is continuing to work on assessing the threat posed by the recent surveillance discovery. IAIP is also studying the interdependencies between the financial sector and other critical infrastructures to determine the interdependencies if any of the targeted institutions are attacked, as well as whether attacks on other critical infrastructure could even more seriously impact the financial sector. The results will be used to identify whether additional protective measures are required.

There are several lessons learned from this current change in threat alert level. As we have experienced in the past, early communications with the affected companies and local law enforcement help private sector security managers and law enforcement develop better coordinated and more effective responses. Prior Site Assist Visits conducted by DHS/IP/PSD at financial sector locations assisted PSD in its outreach to communicate the ORANGE threat level actions to mitigate the threat. Specific information had been shared with the private sector and local law enforcement on attack methods previously employed by terrorist groups and the specific actions needed to mitigate or disrupt potential attacks. This enabled the targeted locations to develop an early warning capability to begin crisis management procedures and implementation of additional appropriate protective measures. IP/PSD teams were deployed to the threatened sites and areas to assist the PFO, liaison with private sector and local law enforcement, and conduct gap analysis, advise on remediation methods and validate that the appropriate protective actions were undertaken.

As I have discussed with you today, IAIP has taken many actions to secure the financial services sector. Our job, however, is not done. We will continue to monitor the evolving threat conditions and communicate even better with the private sector. Together with the Department of the Treasury, we have laid the foundation for a true partnership with the public and private sector. Based on this foundation, and with continued dedication, we will continue to work to protect our Nation.

Again, thank you for the opportunity to testify before you today. I would be pleased to answer any questions you have at this time.

Testimony of
John R. Mohr
Executive Vice President
The Clearing House Association L.L.C.
U. S. House of Representatives
Committee on Financial Services
September 8, 2004

My name is John Mohr and I am an Executive Vice President of The Clearing House which is headquartered in New York. It is the oldest and largest clearing house in the United States and is owned by 19 very large global, international and regional banks. Founded in 1853, The Clearing House is a private-sector, global payment systems infrastructure that clears and settles more than $1.5 trillion per day. It also serves as an industry forum addressing strategic and regulatory issues dealing with payments made in U.S. dollars.

The Clearing House serves more than 1,600 U.S. financial institutions and manages payment services that span the entire spectrum of paper, paper-to-electronic, and electronic payments. Services include local and regional check exchange and settlement services; ACH association and operations; large-value "wire" payments; electronic check presentment; and check image exchange. Financial institutions of all sizes benefit from this unique blend of payment systems that meet the highest standards for reliability, security and service.

I want to thank you for this opportunity to update you about steps which we have taken

to further strengthen the key elements of the U.S. payments infrastructure which are operated by The Clearing House.

One of the key lessons learned from the 9/11 disasters was that from a business continuity perspective "business as usual" was no longer adequate. Contingency and business continuity plans needed to be re-evaluated and refocused.

A major part of the original mission of The Clearing House was to "...promote the interests of its members and to maintain conservative banking through wise and intelligent cooperation." Safety and soundness of the payment system has always been, and continues to be, part of the mission of The Clearing House, and one of our highest priorities.

One of the key reasons our large value payment system, CHIPS, was developed was to address the risk of high-value paper payments. As electronic payments became increasingly important to banks and their customers, TCH focused on the resiliency of its electronic systems. Over the years, TCH has developed a long-standing reputation for producing and managing high-quality software and observing conservative operating practices. TCH was among the first in the industry to operate fully redundant backup sites equipped with uninterruptible power supply (UPS) systems and diesel generators. And the results of these efforts speak for themselves - CHIPS has operated at the highest levels of systems availability since the early 1980's with system availability at or above 99.9%.

Since Sept. 11, 2001, the financial industry has increased its focus on the resiliency of its high-value payments systems. It is universally agreed that systems such as Fedwire and CHIPS must be capable of resuming full capacity operations quickly, within hours of any catastrophe. This is because of the reliance that the financial market places on the high value payments systems for intra-day liquidity and final settlement of their transactions. Without high value payments to "grease the wheels", most financial markets would quickly grind to a halt.

TCH takes this responsibility seriously. It is worth noting that CHIPS never skipped a beat on Sept. 11, and the days that followed. CHIPS itself operated without interruption during the entire crisis and all of the 56 banks that connect to it were able to continue to conduct business. This included the 19 banks that were located in or near the World Trade Center. Each of these banks was required to relocate their operations to their contingency sites in the middle of an unimaginable disaster. The fact that this was successfully accomplished is a great testament to the leadership in these banks.

Following Sept. 11, TCH management reviewed the events of that week for lessons learned. We then reviewed our operations with those lessons in mind looking for ways to improve on the way that we conduct our business. We added additional security staff to perform more frequent and random patrols of our facilities. In addition, a private firm was hired to try to break into our physical and electronic security systems. Based upon findings from those penetration tests, we reconfigured one of our facilities and

implemented state-of-the-art biometric access controls. We implemented an ongoing testing program in place that includes periodic attempts to penetrate our systems to ensure that we maintain high levels of security. We also all but eliminated visitor access to our operating centers.

We reviewed where our critical employees work and relocated some of these individuals to avoid concentration of our workforce and to ensure that the talent needed to maintain and manage our operations is available in the event that we lose one of our sites. We have taken measures to ensure that key operations and support staff have secure remote access to our electronic systems for remote support. In addition, these individuals have Government Emergency Telecommunications Service (GETS) cards which allow them priority access to the public switched network in times of crisis.

For many years, TCH has operated fully redundant data centers, with each capable of backing up the other. All transactions are instantaneously replicated in the backup data center over a private fiber optic ring that interconnects the sites. In addition, CHIPS has customized software that constantly monitors the communications switches of its telecommunications providers and allows for rapid, automatic switching to the backup site. A switch from the primary operations site to the backup site can be accomplished in less than 5 minutes.

To further enhance its resiliency, TCH has developed an out-of-region tertiary data center. This new center is fully equipped to take over operation of CHIPS within an hour

of a simultaneous failure of the other two CHIPS data centers. Using custom mirroring software that was specially developed by The Clearing House, CHIPS was able to conquer the distance limits of synchronous mirroring technology and achieve recovery times consistent with synchronous mirror sites.

Mandatory testing of contingency capabilities has been conducted by CHIPS since the early 1980's. Requirements for mandatory testing and participant backup systems are incorporated into the rules that govern the operation of CHIPS. All users of CHIPS must agree to these rules as a condition of participation in the system. Backup capabilities are tested with the CHIPS community on a quarterly basis. The tests cover a variety of disaster scenarios and exercise the backup and recovery capabilities of the participants, as well as CHIPS. The performance of each participant during these tests is evaluated by The Clearing House and those banks that fail the test are required to continue to retest until they pass. The discipline of regular testing helped contribute to the quick recovery of the banks following the events of 9/11.

Resiliency cannot be achieved in isolation. Global cooperation among all the high-value payment system participants is essential. TCH understands this and actively participates in a number of industry groups dedicated to promoting the resiliency of this critical financial infrastructure. TCH is a member of the SWIFT Resiliency Advisory Council (RAC). In addition, TCH is a member of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security – a public/private group that advises the US Treasury and Dept of Homeland Security on matters of critical

infrastructure protection. TCH also works closely with Fedwire to explore ways to further develop best practices for sound operations and cross-system backup and testing.

When it comes to the safety and soundness of the global payments system, The Clearing House never rests. Backed by its Owner Banks – many of whom are leading experts in the payments industry, TCH promotes the cause of conservative banking practices through the development of best practices, expert commentary on banking regulation and policy and impeccable operations.

Another significant initiative led by The Clearing House following the events of 9/11 was our "Intercept Forum" which addressed the question "What could financial institutions, working with the public sector, do to eliminate the flow of funds to terrorists and their organizations?" We had senior representatives from 34 public and private sector organizations (see attached list). This forum identified five task groups which were co-lead by representatives from both the public and private sectors. These groups and their missions were:

Patterns of Behavior, whose mission was to identify the patterns of behavior of terrorists' funding so that proactive steps may be taken to diminish and ultimately eliminate the flow of funds to terrorists.

Control List, whose goal was to review and confirm that existing and new policies, processes and requirements for obtaining and gathering information about suspected

terrorists and reporting that information to the appropriate government agencies are in place and working appropriately.

Account and Transaction Monitoring was charged with developing procedures and policies to identify and monitor transactions and/or account opening activity related to terrorist activity.

Global Cooperation and Best Practices focused on issues beyond our borders. It was clear that making changes only in the U.S. would simply drive terrorist financing to other countries. Therefore this team worked globally to remove obstacles to the flow of information needed to counteract terrorist financing and to export "Best Practices" to cooperating countries.

The **Database** team had a mission to develop a highly secure, real-time capability for regulatory and law enforcement agencies to download suspected terrorists/terrorist organizations "identities" to financial institutions seeking account and/or transaction hits which in turn would be uploaded to the respective agencies.

The Intercept Forum is a great example of the private and public sectors' ability to work together to achieve shared goals. Financial institutions, law enforcement agencies and regulators were able to draw upon each other's core competencies in a cooperative way and achieve meaningful results. It is clear that going forward we will need continued cooperation in all three areas in order to be successful.

Attachment A

Clearing House Owners

The Clearing House is owned by the following banks or their U.S. commercial banking affiliates: ABN AMRO Bank, Bank of America, The Bank of New York, Bank of Tokyo-Mitsubishi/Union Bank of California, BB&T, Citibank, Citizens Bank, Comerica Bank, Deutsche Bank, HSBC Bank, JPMorgan Chase Bank, KeyBank, M&T Bank, National City Bank, PNC Bank, SunTrust Bank, U.S. Bank, Wachovia Bank, Wells Fargo Bank.

Attachment B
Intercept Forum
Participating Organizations

Financial Institutions
ABN AMRO
Bank of America, N.A.
The Bank of New York
Bank One, N.A.
Citibank, N.A.
Deutsche Bank
FleetBoston
HSBC Bank
J.P. Morgan Chase & Co
Wachovia
Wells Fargo
Goldman Sachs

Associations
American Bankers Association (ABA)
American Council of Life Insurers (ACLI)
American Insurance Association (AIA)
New York Clearing House (NYCH)
Securities Industry Association (SIA)

Government Agencies
Department of Justice
Federal Bureau of Investigation (FBI)

Federal Deposit Insurance Corporation (FDIC)
Federal Reserve System, Washington, D.C. (FRB DC)
Federal Reserve Bank of New York (FRBNY)
Financial Crimes Enforcement Network (FinCEN)
New York State Banking Department
Office of Comptroller of the Currency (OCC)
Office of Foreign Assets Control (OFAC)
Office of Thrift Supervision (OTS)
Secret Service
Securities and Exchange Commission (SEC)
U.S. Attorney's Office, Southern District, New York
U.S. Department of the Treasury

Other
Sullivan & Cromwell
Depository Trust & Clearing Corporation (DTCC)
FDC/Western Union

For release on delivery
10:00 a.m. EDT
September 8, 2004

Statement of

Mark W. Olson

Member

Board of Governors of the Federal Reserve System

before the

Committee on Financial Services

U.S. House of Representatives

September 8, 2004

Introduction

Thank you Chairman Oxley and Ranking Member Frank, for inviting me to discuss a matter of significant importance to our country: protecting our financial infrastructure. As we approach September 11, I would like to take a moment to honor the memory of those who lost their lives and to honor those who supported one another on September 11, 2001.

Although the financial sector has years of experience dealing with operational disruptions caused by weather, power, and other critical infrastructure outages, the September 11 attacks had a profound effect on how the industry thinks about physical and cyber security as well as business-continuity planning. After the crisis subsided, sector participants, including the Federal Reserve, reflected on lessons learned and how they should be incorporated into daily business processes and business-resumption planning.

My remarks today will highlight the actions the Federal Reserve took on September 11 and immediately following to maintain confidence in and restore the operation of our financial system. I will also focus on numerous steps that we and the other financial regulators have taken since September 11 to improve the resilience of--and to protect--the financial infrastructure.

Response to September 11

On Tuesday, September 11, terrorists destroyed a portion of the critical infrastructure that supports the U.S. financial markets, disrupted communications networks, and forced numerous market participants to move to contingency sites. These challenges, along with the tragic loss of employees of a few major financial firms, complicated trading, clearing, and settlement of a number of financial instruments. Operational disruptions caused uncertainties about payment flows, making it difficult for the reserve market to channel funds to where they were needed most. Depository institutions that held more reserve balances than they preferred had difficulty

placing and delivering the excess in the market; on the other hand, depository institutions awaiting funds had to scramble to cover overdraft positions. As a result, market participants experienced significant liquidity dislocations, and the demand for reserves grew rapidly.

The Federal Reserve accommodated the demand for reserves through a variety of means, the relative importance of which shifted through the week. On Tuesday morning, shortly after the attacks, the Federal Reserve issued a press release stating that "the discount window is available to meet liquidity needs," thus reassuring financial markets that the Federal Reserve System was functioning normally. Borrowing by depository institutions surged to a record $45.5 billion by Wednesday. Federal Reserve discount loans to banks to meet liquidity needs dropped off sharply on Thursday and returned to lower levels by Friday. Separately, overnight overdrafts on Tuesday and Wednesday rose to several billion dollars, as a handful of depository and other institutions with accounts at the Federal Reserve were forced into overdraft positions on their reserve accounts. Overdrafts returned to negligible levels by the end of the week.

Like their U.S. counterparts, foreign financial institutions operating in the United States faced elevated dollar liquidity needs. In some cases, however, these institutions encountered difficulties positioning the collateral at their U.S. branches to secure Federal Reserve discount window credit. To be in a position to help meet the enhanced need for funds, three foreign central banks established new or expanded arrangements with the Federal Reserve to receive U.S. dollars in exchange for their respective currencies. These swap lines, which lasted for thirty days, consisted of $50 billion for the European Central Bank, $30 billion for the Bank of England, and an increase of $8 billion (from $2 billion to $10 billion) for the Bank of Canada. The European Central Bank drew on its line that week to channel funds to institutions with a need for dollars.

During that week, the disruption in air traffic caused the Federal Reserve to extend record levels of credit to depository institutions in the form of check float. Float increased dramatically because the Federal Reserve continued to credit the accounts of banks for the checks they deposited, even though the grounding of airplanes meant that checks normally shipped by air could not be presented to the checkwriters' banks on the usual schedule. Float declined to normal levels the following week once air traffic was permitted to recommence. Finally, over the course of the week, as the market for reserves began to function more normally, the Federal Reserve resumed the use of open market operations to provide the bulk of reserves. The open market desk accommodated all propositions for funding through repurchase agreements down to the target federal funds rate, operating exclusively through overnight transactions for several days. The injection of reserves through open market operations peaked at $81 billion on Friday. The combined infusion of liquidity from the various sources caused the level of reserve balances at Federal Reserve Banks to rise to more than $100 billion on Wednesday, September 12--about ten times the normal level.

In addition to accommodating the heightened demand for reserves, the Federal Reserve took several steps to facilitate market functioning in the wake of the September 11 attacks. For example, the hours of the funds and securities transfer systems for U.S. government and agency securities operated by the Federal Reserve were significantly extended during the week after the attacks. From September 11 through the 21st, the Federal Reserve reduced or eliminated the penalty charged on overnight overdrafts, largely because those overdrafts were almost entirely the result of extraordinary developments beyond the control of the account holders. For four weeks after the attacks, the Federal Reserve Bank of New York liberalized the terms under which it would lend securities from the System portfolio, and the amount of securities lent rose

to record levels in the second half of September. The Federal Reserve working with the National Communications System (NCS) also assisted market participants in restoring their telecommunications services.

The markets and financial market authorities worked hard to restore operations, and market activity resumed relatively quickly after the attacks. By the week following September 11, the financial system had largely begun to function normally, although activities to address the aftermath of the attacks continued for some time.

Steps Taken Since September 11 to Protect the Financial Infrastructure

Within weeks of September 11, we initiated a self-assessment of our contingency arrangements across the Federal Reserve and embarked on forty initiatives, which we classified under five broad headings:

- Ensure continuity of Federal Reserve operations.
- Ensure market liquidity during a crisis.
- Ensure effective communications and coordination during a crisis.
- Improve resilience of the private-sector financial system infrastructure.
- Improve resilience of the telecommunications infrastructure supporting critical financial services.

Some of the key steps the Federal Reserve has taken to improve our own infrastructure and our delivery of critical central-bank and financial services include the following:

- We have developed plans to ensure that critical central-bank activities, supervisory functions, and financial services operations have sufficient redundancy in facilities and staff. We have enhanced and tested business-continuity arrangements for critical functions and business lines.

- Our facilities for providing critical financial services are backed up at fully operational, geographically diverse sites to ensure a speedy recovery even if the critical infrastructure is disrupted across multistate areas.
- We have enhanced our resiliency for discount window lending and cash services provided by the Reserve Banks.
- We have improved our tools and authority to provide liquidity in a crisis. In 2003, the Board established the primary credit program, as well as special arrangements for rapidly reducing the primary credit rate to the federal funds rate in an emergency. We also have improved the ability of the Board to approve the extension of emergency discount window credit.

The federal financial agencies took immediate steps to work together to identify new vulnerabilities exposed by September 11. These efforts were coordinated under the umbrella of the President's Working Group on Financial Markets, the Financial and Banking Infrastructure Information Committee (FBIIC), and, for depository institutions more specifically, the Federal Financial Institutions Examination Council (FFIEC). The agencies have implemented a duty officer program and developed communications protocols for dealing with their staffs, regulated financial institutions, and the public. We have also developed and tested facilities for secure communication among ourselves and with other agencies.

The agencies that participate in FBIIC, including the Federal Reserve, and that have direct supervisory and regulatory responsibilities for the financial sector have assessed potential system vulnerabilities. We have shared that information with the Department of Homeland Security (DHS). Indeed, I would like to commend the DHS the for their work to share

information and coordinate with the financial sector including the FBIIC during the recent elevation of the threat level to orange for financial services firms in New York City, northern New Jersey, and Washington, D.C. The timely communications and sharing of information enabled financial-sector participants and law enforcement authorities to take steps to mitigate risks so that customers or financial services firms were able to conduct business in the usual fashion. Financial-sector participants, including the financial regulators, strengthened business-resumption plans with an overall goal of ensuring the smooth operation of the financial system. Previously, terrorist attacks were treated as low-probability/high-impact events affecting a single institution. As a result of September 11, industry participants are now planning for events that affect wide areas, last longer, and involve loss of life or widespread destruction of property and information assets.

The process of strengthening the resilience of the financial system and, in particular, organizations that could have a systemic effect if they were disabled, is being accomplished through the existing regulatory framework. More than a year ago, in April 2003, the Federal Reserve, the Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission (SEC) issued an *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*. The paper formalizes a set of sound practices viewed as necessary by the agencies and the financial industry to ensure the rapid recovery of the U.S. financial system following a wide-scale disruption that may include loss or inaccessibility of staff. In particular, the paper articulates sound practices for resumption and recovery of critical clearing and settlement activities by core clearing and settlement organizations and financial institutions that play significant roles in critical markets by virtue of their market share (greater than five percent in one or more critical financial markets). The sound practices include establishing

geographically dispersed backup facilities for clearing and settlement so that these organizations can meet recovery objectives within the business day if a wide-scale disruption takes place.

Using their respective supervisory and regulatory processes, the agencies are conducting focused, ongoing dialogues with the organizations that are subject to the sound practices paper. Financial organizations are investing millions of dollars to implement the sound practices. Clearing and settlement organizations, which are the financial utilities for the U.S. financial system, have made substantial progress in improving their resilience and achieving out-of-region geographic dispersion between primary and backup operations facilities and data centers. Several have met or will meet the sound practices by year-end, with the remainder scheduled to complete implementation in the second half of 2005. Banks and broker-dealers that play significant roles in the critical markets defined in the paper indicate they will meet the paper's 2006 implementation date.

The sound practices are also relevant to other financial-sector participants. Many of the concepts in the paper amplify long-standing and well-recognized principles relating to safeguarding information and the ability to recover and resume essential financial services. Over the past few years, the FFIEC has revised and expanded guidance for banking organizations pertaining to operational risk. In December 2002, we issued revised guidance on information security. In April 2003, the FFIEC issued expanded guidance on business-continuity planning. The guidance addresses both the operational- and business-risk issues that depository institutions must incorporate into their business-continuity plans. The guidance specifically refers to the need to plan and test for recovery of critical business lines and functions--such as retail banking services--in the face of wide-scale disruption, as well as scenarios in which physical or information assets and personnel are lost. Recently, the FFIEC issued guidance on managing

additional risks arising from information technology operations, network management, and wholesale and retail payments systems. Our examiners are assessing banks against these guidelines. Other financial market authorities are taking similar steps for the organizations that they regulate.

Challenge of Protection

While the agencies and financial-sector participants are working to improve their operational resilience, some vulnerabilities continue to pose challenges. The strategy underlying the sound practices is to increase the likelihood that systemically critical institutions will be able to recover rapidly from a wide-scale disruption. However, the sound practices address only recovery, not the prevention of an attack.

The agencies are addressing this concern by working to improve coordination and emergency planning efforts between federal, state, and local homeland security authorities; the various federal, state, and local protection agencies; and the systemically critical institutions. Efforts have focused on the locations where the systemically critical institutions have their primary operations--including New York City. The agencies also plan to work with local protection agencies in cities where critical institutions are locating backup sites. As part of these efforts, the Department of the Treasury has arranged for site surveys of key financial-services sector assets to determine whether physical security can be hardened. Protection plans have been developed and are being implemented.

Importance of Telecommunications to the Financial Services Sector

The resilience of the telecommunications infrastructure is, from our perspective, one of the most important national issues involving the nation's critical infrastructure. The U.S. financial system depends on telecommunications to effect transactions and make payments.

Following September 11, the Federal Reserve and the FBIIC agencies expanded and promoted the use of National Security/Emergency Preparedness (NS/EP) telecommunications programs sponsored by NCS. These programs worked well in helping to resume operations on September 11. The Federal Reserve is working with FBIIC agencies through outreach to expand NCS services to clearing and settlement organizations processing securities. Approximately 5,000 additional authorizations to ensure the priority of voice telecommunications have been issued in the financial sector. Moreover, about 4,100 critical circuits used to transmit financial data have been registered for priority restoration and provisioning of new lines; these include most circuits between the payment and settlement systems, the markets, and key market participants.

The National Security/Emergency Preparedness telecommunications program operated by the NCS currently focuses on recovery and restoration. The FBIIC agencies believe that a third aspect-- protection--through establishment of a national program for maintaining physically diverse circuits and switches, should be incorporated into the program. Treasury has designated the Federal Reserve as the lead agency for telecommunications in the FBIIC as an interdependencies study. At the Federal Reserve's request, the telecommunications sector through the National Security Telecommunications Advisory Committee (NSTAC) reviewed the resilience of the telecommunications infrastructure. In response to the NSTAC's recommendations that were submitted to the President in April 2004, the Alliance for Telecommunications Industry Solutions (ATIS) is organizing a National Diversity Assurance Initiative. ATIS has asked the Federal Reserve to participate in a pilot program to develop and test the requirements for physical circuit diversity across multiple carriers that can be used by the financial system and potentially other critical sectors. The Federal Reserve is collaborating with

telecommunications services providers through NSTAC and the Federal Communications Commission Network Reliability and Interoperability Council. As an example, the Federal Reserve is currently working with the NSTAC to plan how NS/EP telecommunications services can be applied to the next generation of telecommunications networks based on internet protocols.

Summary

In summary, Mr. Chairman, we believe that protecting the infrastructure that supports our financial system is a matter of national importance. As a result of careful planning and considerable investment by both the private and public sectors, the financial sector is one of the most resilient parts of our economy. The supervisory framework for the financial sector oversees compliance with security and business-resumption expectations, which are relatively high because of the importance of ensuring the smooth operation of our financial system. All financial institutions have been expected to incorporate lessons learned from September 11, recent power outages, and cyber attacks. Organizations that we believe could have a systemic effect on the financial system if their functions were disrupted are being asked to meet very high standards of business resumption. The Federal Reserve will continue to treat the protection and resilience of the sector as a key responsibility.

Thank you Mr. Chairman and members of the Committee. I am happy to respond to any questions.

ChicagoFIRST

Chicago Financial Services Industry Coalition
for Business Continuity

Testimony
of
Brian S. Tishuk
Executive Director
ChicagoFIRST

before the

U.S. House Financial Services Committee

on

Protecting our Financial Infrastructure:
Preparation and Vigilance

September 8, 2004

Written Testimony of Brian S. Tishuk, Executive Director, ChicagoFIRST
September 8, 2004

Good morning. Chairman Oxley, Ranking Member Frank, and Members of the Financial Services Committee, I am Brian Tishuk, the Executive Director of ChicagoFIRST. I am honored to appear before this Committee and to be part of this distinguished panel. Chicago's leading financial institutions comprise our organization, through which they cooperate with one another and collaborate with government to address common business continuity and homeland security issues.

In my statement, I will discuss how regional public/private partnerships can enhance the resiliency of financial institutions and how ChicagoFIRST, as such an entity, can be replicated across the nation.[1]

Introduction

I became the first Executive Director of ChicagoFIRST in February of this year. This followed a 19-year career at the Treasury Department, where I addressed financial institutions issues of all kinds within Financial Institutions Policy. Following the horrific events of September 11, 2001, I established and led the Department's Office of Critical Infrastructure Protection and Compliance Policy (CIPCP), which focused on: critical infrastructure protection and homeland security; money laundering and terrorist financing; and the security of personal financial information.

Before explaining the activities that we have undertaken within ChicagoFIRST, I would like to first explain the need for regional partnerships and how the basic structure and approach of our organization serves as a model for financial institutions in other areas of the country.

Regional Partnerships

Natural disasters, terrorist attacks, and other crises happen locally and affect the region in which they occur most acutely.

[1] A list of our members and strategic partners is appended to this statement.

Government takes the necessary steps to prevent intentional acts, respond to a disaster, and to recover. Private institutions establish security protocols to prevent and thwart intentional acts, and they develop and implement business continuity and disaster recovery plans.

These are necessary, but insufficient, steps to protect the people who comprise the most important asset of financial institutions. Financial institutions must ensure that their plans do not conflict with those of their counterparts and that they will mesh well with governmental plans for prevention, response, and recovery. For example, if a firm's evacuation plan calls for employees to head south to a park, that firm should not find out in the midst of a crisis that the city will order its employees north to an alternate location. It would also be an inauspicious time to learn that, while the firm's building is safe, yellow tape prevents essential employees from reentering the facility to resume critical operations. The global reliance on U.S. financial markets renders such a situation completely unacceptable for financial institutions.

Engaging local and state governments to discuss evacuation procedures, credentialing, sheltering in place and other issues can best be accomplished through a regional partnership, such as ChicagoFIRST. The public sector will be overwhelmed if each institution seeks to cover the same ground individually, possibly with conflicting and inconsistent solutions. Financial institutions will be much stronger, and far more successful, working together.

That ChicagoFIRST is unique within the financial sector attests to the difficulty of forming a regional partnership. Yet, such efforts are necessary for the protection of critical financial infrastructure. We believe that the federal government should more actively promote and support efforts to form and sustain organizations like ChicagoFIRST in financial centers. The Treasury Department and the Department of Homeland Security (DHS) have contributed to our success. However, these agencies need to do more to draw financial institutions into the homeland security effort through these partnerships.

The Treasury Department, as the financial sector's lead agency, has a solid and respected record of applying its varied resources to benefit the sector. However, we believe it should bolster its efforts to

increase private sector awareness of the work of the Financial and Banking Information Infrastructure Committee (FBIIC), composed of all relevant federal financial regulators, the Financial Services Sector Coordinating Council (FSSCC), a private sector organization that coordinates with FBIIC, and the Financial Services Information Sharing and Analysis Center (FS-ISAC), an private sector information sharing organization. Knowledge of these resources would help financial services institutions throughout the country understand that they will not be going it alone as they work to form partnerships to increase their resiliency in the face of potential disasters.

The Department of Homeland Security (DHS) also has a role to play. Its regional arms, such as the Federal Emergency Management Agency and the United States Secret Service, can provide regional partnerships tremendous value and assistance, as they have done for ChicagoFIRST. DHS's Private Sector Office can also support and facilitate regional partnerships, as that Office, too, has done with ChicagoFIRST. However, the Department as a whole needs to take more of an initiative in reaching out to financial institution centers and promoting regional partnerships.

Federal agencies and national organizations cannot organize regional partnerships, but their assistance in working with state and local government, financial institutions, and others can prove invaluable.

Founding ChicagoFIRST

The Chicago financial services industry is the most diverse in the United States. Its participants include securities and futures exchanges, large and small banks, securities and futures clearinghouses, and check clearing and cash operations by the Chicago Federal Reserve Bank. The financial services industry is one of the largest employers in the City of Chicago. Because of its diversity, disruption of these markets would seriously affect key operations across the country.

In light of the events of September 11, each of the members of the Chicago financial services community reexamined and enhanced its individual business continuity plan to increase its ability to survive such an event. As this work proceeded, many institutions came to

realize that the utility of each firm's individual plan depended on the emergency preparedness of the City of Chicago and the State of Illinois.

During the summer and fall of 2002, two third-party efforts sought to coordinate the Chicago financial community. Although institutions saw the benefit of organizing, it became clear that they preferred to organize themselves, rather than to be coordinated by an outside party.

Treasury Department officials visited Chicago in March 2003 and encouraged the members of the financial services industry to work together on business continuity issues. They also met with the head of the City of Chicago's new Office of Emergency Management and Communications (OEMC), stressing the importance of the financial services industry and the need for the OEMC to work with the industry.

Informal discussions among Chicago financial institutions in April 2003 led to the realization there were a number of common questions and concerns about the emergency plans of the City of Chicago and the State of Illinois. They also shared a sense of frustration that answers were hard for them to obtain individually.

In May 2003, a number of the leading financial institutions determined that it would be productive to form an organization to address regional business continuity issues in partnership with the city, state, and federal government. Louis Rosenthal, Executive Vice President, LaSalle Bank, and Ro Kumar, First Vice President, The Options Clearing Corporation, now co-Chairs of ChicagoFIRST, took the lead at the meeting. They presented a draft mission statement and draft primary objectives for a potential new organization that they called ChicagoFIRST. Active discussion by the industry participants at the meeting refined the drafts, which led to an agreement to form ChicagoFIRST as an informal coalition.

Mission and Objectives of ChicagoFIRST

The mission and primary objectives agreed to in May 2003 continue to guide ChicagoFIRST today.

The mission of ChicagoFIRST is to increase the resilience of the Chicago financial community in collaboration with the city, state, and federal agencies, including to: (1) protect the lives of the thousands of people who work in the industry; (2) protect the financial assets that have been entrusted to it for safekeeping and investment; and (3) implement the primary objectives of the organization expeditiously.

The primary objectives were to: (1) obtain a seat at the OEMC's Joint Operations Center (JOC) in the event of a crisis that affects Chicago's financial community; (2) develop and communicate standard evacuation procedures for industry personnel to exit the city if necessary; (3) create permits/passes for essential personnel to enter business facilities that are safe, but to which access is restricted (credentialing); and (4) increase the understanding of city and state emergency management administrators about the criticality of the local financial services industry.

In July 2003, the formation of ChicagoFIRST was announced at a press conference attended by representatives of the organization, the OEMC, and the Department of the Treasury. The Department lauded ChicagoFIRST as "a useful model that may serve other communities well."[2] The participants at the news conference stressed that collaboration between the private and public sectors was necessary to protect the Chicago financial services community. ChicagoFIRST also announced that it would initially be supported by BITS, a technology and business strategy group consisting of the top 100 financial services companies in the U.S. BITS' role was to support implementation of ChicagoFIRST's primary objectives and to recommend an ongoing structure for the coalition.[3]

---

[2] Joint Press Release of the Department of the Treasury, City of Chicago's Office of Emergency Management and Communications, and ChicagoFIRST (July 10, 2003) (quote of Michael Dawson, Treasury Deputy Assistant Secretary for Critical Infrastructure Protection and Compliance Policy).

[3] As a condition of assisting ChicagoFIRST, BITS was permitted to produce a paper outlining the manner in which the ChicagoFIRST experience could be replicated elsewhere. With the assistance of the Treasury Department, which hired the Boston Consulting Group to collaborate with BITS and ChicagoFIRST, a final document is expected to be published soon.

In January 2004, 14 members formed ChicagoFIRST as a legal entity and hired me. Assistant Secretary Abernathy fully supported these developments, considering them means of both furthering the goals of ChicagoFIRST and Treasury's interest in developing other regional partnerships within the financial sector.

Progress on the Primary Objectives of ChicagoFIRST

Thanks to the tireless efforts of volunteers from ChicagoFIRST's members and the invaluable assistance of our strategic partners, important progress has been made on all of ChicagoFIRST's primary objectives. However, much remains to be done.

ChicagoFIRST's most important objective was to obtain a seat at the OEMC's JOC. The JOC includes seats for a number of city agencies that would be involved in a regional disaster, including the police, fire department, sanitation department, and public health department. ChicagoFIRST's members wanted a seat at the JOC to gain and share information in times of emergency in order to protect employees and businesses. OEMC agreed to give ChicagoFIRST a seat at the JOC in July 2003. Staff from the members of ChicagoFIRST and from the Federal Reserve Bank of Chicago will occupy the seat if necessary. A rotation schedule has also been devised.

Developing and communicating standard evacuation procedures has proven to be a more complicated project than the members of ChicagoFIRST initially thought. The city and state are both working together and with ChicagoFIRST, but we have found that our mutual assumptions require further analysis and lengthy discussion. Moreover, the city can share only so much of its plans, because it needs to preserve its flexibility in times of emergency and is concerned that revealing evacuation plans too widely could jeopardize security.

However, useful progress has been made. Just last month, ChicagoFIRST was privileged to be one of very few private sector entities to participate in a tabletop sponsored by the Illinois Department of Transportation and the Illinois Emergency Management Association, with active participation by the OEMC and numerous city agencies. This exercise revealed that some of the assumptions underlying the business continuity plans of many of our members might conflict with the assumptions underlying the evacuation plans of

the city. ChicagoFIRST continues to work through these issues with the city in a spirit of partnership.

ChicagoFIRST is also working with the city and the Red Cross to develop plans for shelter-in-place protocols for employees. Jointly, we will devise guidance on these protocols and train ChicagoFIRST employees on shelter-in-place best practices.

Steady progress has been made toward a credentialing system that would allow essential personnel to access closed buildings or areas of the city when it is safe to do so after a regional disaster. ChicagoFIRST and the city are using an interim credentialing solution while a permanent credentialing system is being developed. The city and state are currently discussing the need for and development of a common credentialing system, a dialogue for which ChicagoFIRST deserves some credit.

With the participation of the Department of the Treasury, ChicagoFIRST held an education briefing for the city in August 2003. The briefing was well attended and well received by city employees, many of whom were first responders with extensive experience in protecting lives and property, but less experience with the financial services industry. ChicagoFIRST members also have made presentations about the organization and its goals to the Illinois Terrorism Task Force. ChicagoFIRST has also reached out to fledgling regional business continuity organizations in Minneapolis and Cleveland.

ChicagoFIRST as the Model for Regional Partnerships

Every regional partnership will necessarily be unique, addressing issues of relevance to a locality in a manner appropriate for the parties involved. Only those agencies and institutions "on the ground" can do this, and financial institutions can do this well only if they organize themselves and leverage their relationship.

Though a product of its own milieu, ChicagoFIRST has been constructed in a manner that would allow its salient elements to be replicated in other parts of the country. I would like to highlight four components of our model that would place any regional partnership in good stead.

Grassroots Leadership

Financial institutions should organize themselves in a grassroots fashion. Only they can articulate the business case and present it credibly to their colleagues and to their public sector partners. Third-party organizers will necessarily operate under a different business model, continuing to lead a partnership only as long as it proves beneficial to them, with the needs of its financial institution members taking an understandably secondary position.

Leadership must come from within the financial institution members. One leader is essential, but having two assures competitors that there is no hidden agenda. Ro Kumar and Louis Rosenthal provided that leadership for ChicagoFIRST, drafting the mission statement and identifying the "low hanging fruit" that helps such a coalition succeed at the outset.

Organization Self-funding

With the critical infrastructure largely in the hands of the private sector, we have an obligation to put "skin in the game," as the saying goes. However, at least in the short term, funding from the public sector must also be provided. I am not saying that government should be expected to fund operating expenses. Doing so will simply invite public control of the organization, which will vitiate the very concept of a partnership.

Nevertheless, there is a role for government assistance. The federal government should help to fund projects that enhance the security of the region and would be difficult, if not impossible, for the partnership to fund alone. The Treasury Department has been very generous with ChicagoFIRST and other financial sector participants in this regard. We believe that DHS should also be supporting regional partnerships, but we have not been completely satisfied with their participation to date.

Build Relationships with Public Agencies

In a general sense, the whole purpose of an organization like ChicagoFIRST is to build relationships with its public partners. This

allows both the public and private sides to know what to expect of one another in a crisis, so that false assumptions will not have to be confronted during the heat of a crisis, but can instead be factored into our respective approaches to such events.

Information sharing derives from such relationships. Although our highest priority was to secure a seat in the Chicago JOC, we knew that much of our information sharing would take place outside of a crisis, and it has. Such sharing ranges from the mundane of our asking the city about a bevy of police/fire/rescue vehicles on the street in a particular location to the essential of having the City of Chicago and the State of Illinois give us a "heads up" about impending issues and announcements, such as the August 1 disclosure of terrorist threats against financial firms in New York City, New Jersey, and Washington, DC.

A regional partnership will neither supplant nor direct the business continuity plans of its individual members; that responsibility remains with them. The core competence of a partnership is to: obtain information from the public sector and to share it with the members; share relevant institution information among the members; and provide the public sector with timely information about financial institutions that protects employees, markets, and the region.

Model Adaptability

Not only can the above elements be replicated elsewhere, but also adapted to any region. For example, the size and importance of the Chicago financial community justifies a partnership where the private sector is exclusively financial. However, those areas of the country that lack a critical mass of financial institutions could adapt this model to a group that includes members from other sectors.[4]

Even if other sectors become members, financial institutions remain fertile ground for leaders and organizers. Being heavily regulated, they find nothing unusual about working with the public sector. More importantly, financial institutions understand keenly the need to reduce operations risk.

---

[4] For example, a partnership in one region is being led by a financial institution, but other members include an electronics store, a retail store, and a manufacturer.

I don't want to underestimate the difficulty of establishing and continuing an organization like ChicagoFIRST. I can assure you that "getting off the ground" is only the beginning of the challenges and expenses. That being said, the members of ChicagoFIRST are committed to making sure that the organization is around for the long haul.

ChicagoFIRST is on the Map

Despite its short history, ChicagoFIRST has been tremendously successful, becoming a fixture of the Chicago financial landscape.

- The City of Chicago has become our most important partner, and we have worked with them on several pilot programs of mutual benefit. In fact, Ron Huberman, the Executive Director of the OEMC, has reached out to ChicagoFIRST and proposed his own agenda for protecting financial markets.

- The Illinois Terrorism Task Force, one of the state's forward-looking homeland security efforts, recognizing the contribution we can make, has invited us to attend regular meetings of the government-focused task force.

- The Illinois State Police have developed an information-sharing conduit for law enforcement called the Statewide Terrorism Intelligence Center. Before rolling it out to certain segments of the private sector, the state police asked ChicagoFIRST to pilot test it. And we are.

- Local media have begun recognizing ChicagoFIRST as a single point of contact for the area's financial community.

ChicagoFIRST has also become part of the landscape of the national financial sector.

- ChicagoFIRST presents at each of the financial sector outreach conferences held by FBIIC and FSSCC. According to the surveys collected after each one, our presentation is valued highly by the attendees as an important best practice.

- ChicagoFIRST joined FSSCC earlier this year, and will host the quarterly meetings of FBIIC and FSSCC next week. This marks the first time that these meetings have been held in a city other than New York or Washington, DC.

- Our presence here today illustrates the progress that we have made in addressing homeland security issues facing Chicago's financial institutions since September 11.

July Tabletop Exercise

I would like to elaborate on the crowning achievement of 2004: a July tabletop exercise that proved successful in every way. Most importantly, we devised a scenario that examined how the partnership would function if financial institutions were forced to operate for an indefinite period of time under the threat of terrorist attack. Two weeks after the event, we saw that very scenario unfold in real life as the Secretary of Homeland Security unveiled terrorist designs against East Coast financial institutions.

The goal of the tabletop, conducted by ChicagoFIRST, in collaboration with the OEMC, and with important financial assistance from the Department of the Treasury, was to test the resiliency of the financial services sector and to improve security in Chicago. Representatives of members of ChicagoFIRST and many of our strategic partners actively participated in this two-day exercise. In all, 21 financial institutions and 17 government agencies attended the exercise. The scenarios that the participants worked through were designed to severely test the plans and communications channels between ChicagoFIRST and its strategic partners.

ChicagoFIRST will meet later this month to examine the lessons learned at the exercise and to develop a plan to address these issues through committees headed by ChicagoFIRST members. Some of those tasks include the following:

- Obtain alternative communication methods, because traditional methods could be damaged during a crisis;

- Strengthen employee preparedness for emergencies, both at work and at home;

- Develop our nascent relationships with the counties in the region, where many of our employees live;

- Institute relationships with telecommunications providers and the utilities; and

- Test, fill gaps, repeat. Our members found the tabletop so valuable that we are firmly committed to the concept of group testing.

Area of Concern

One of my former colleagues was fond of asking those involved in homeland security efforts what kept them awake at night. If posed to me, I would give the following answer:

- As identified threats lead to the hardening of financial institutions and metropolitan areas on the East Coast, terrorists will look for financial targets perceived to be softer. We do not want Chicago to be seen as such a target.

- We have mentioned to DHS our interest in hardening Chicago generally and the financial district specifically. Among other things, we seek: funding for certain safety equipment sought by both the city and ChicagoFIRST; placing a DHS regional center in Chicago; and procuring security clearances for key financial representatives so that deeper collaboration between the public and private sectors can occur.

To date, we have not received answers to these inquires from DHS. We hope that our appearance here today will be the beginning of a relationship with that agency as productive as those we have with the City of Chicago, the State of Illinois, and the Treasury Department.

Conclusion

The members of ChicagoFIRST are very proud of our progress. We have a very productive relationship with the City of Chicago, the State of Illinois, and the Department of the Treasury and law enforcement at all levels. While much remains to be done, the members of ChicagoFIRST are confident that the financial services

community of Chicago is better prepared to protect its employees and businesses in the event of a regional disaster than we were before ChicagoFIRST was formed. We hope that our successful approach can provide a model for private/public partnerships in other cities throughout the country.

Thank you again for the opportunity to testify at this important hearing. I would be happy to answer any questions that you have.

MEMBERS OF CHICAGOFIRST

ABN AMRO/LaSalle Bank
Allstate Insurance Company
Archipelago
Bank of America
Bank One
Chicago Board Options Exchange
Chicago Board of Trade
Chicago Mercantile Exchange
Chicago Stock Exchange
Harris Bank
Mesirow Financial
Mizuho Securities USA
Northern Trust
The Options Clearing Corporation
UBS
William Blair & Company

STRATEGIC PARTNERS OF CHICAGOFIRST

Chicago Electronic Crimes Task Force (United States Secret Service)
Chicago Police Department 1st District - Central
City of Chicago Office of Emergency Management and Communications
Commodity Futures Trading Commission
Federal Bureau of Investigation/InfraGard – Chicago Chapter
Federal Deposit Insurance Corporation
Federal Emergency Management Agency, Region V
Federal Reserve Bank of Chicago
Financial and Banking Information Infrastructure Committee
Financial Services Information Sharing and Analysis Center
Financial Services Roundtable/BITS
Financial Services Sector Coordinating Council
Futures Industry Association
Illinois Department of Financial and Professional Regulation
Illinois Emergency Management Agency
Illinois Terrorism Task Force
Office of the Comptroller of the Currency
Securities and Exchange Commission – Division of Market Regulation
State of Illinois
United States Attorney's Office, Northern District of Illinois
United States Department of Homeland Security, Private Sector Office
United States Department of the Treasury, Office of Critical Infrastructure Protection

New York Stock Exchange Response to questions posed by Congressman Ruben Hinojosa (D-TX) after the Financial Services Committee hearing entitled, "Protecting Our Financial Infrastructure: Preparation And Vigilance."
September 8, 2004

1. For Robert Britz, Co-Chief Operating Officer, NYSE:

"You mention in your testimony that the New York Stock Exchange recently received approval to establish a remote National Market System data center.
You also note that the center will likely be ready sometime in 2005. I am going to ask you a two-part question:

a. "Will the data center be manned 24/7, or will it just be available to be brought on-line should terrorists attack again?"

The New York Stock Exchange did not receive approval to establish a remote National Market System data center. The Consolidated Tape Association/Consolidated Quotation Operating Committee (CTA/CQOC) directed the Securities Industry Automation Corporation (SIAC), of which I serve as Chairman, to move one of the National Market System data centers away from the New York area. SIAC designed and is currently implementing a remote data center for them in support of the Consolidated Tape and Consolidated Quotation (CT/CQ) systems, and for the Options Price Reporting Authority
("OPRA") in support of the OPRA system.

The data center will normally be operated remotely, and minimal on-site manpower is required. Our systems are designed so the operators do not have to be collocate with the computers.

The remote data center will be on-line and will be sharing the daily processing load with the primary data center.

In the event that neither our primary nor our remote operations centers are capable of functioning, we would staff the National Market System remote data center to monitor and operate the Consolidated Tape System, Consolidated Quotation System and the Options Price Reporting Authority systems directly from this remote data center.

b. "How far from Wall Street will data center be located? I ask the second part of this question because several brokerage houses expressed concern in the past that it would be very expensive for them to have alternate sites located far from New York City."

The data center will be located approximately four to five hours driving time from New York City.

Governor Olson subsequently submitted the following in response to written questions received from Congressman Spencer Bachus in connection with the September 8, 2004, hearing before the Committee on Financial Services:

Q. I continue to believe that contingency measures and business continuity planning are better suited to manage operational risk than the operational risk-based capital charge proposed by the Basel Committee. It is my understanding that bank regulators have gone ahead and put in literally thousands of hours on operational risk portion of the new Basel Capital Accord. Does it make sense for the Federal Reserve to dedicate such resources to an operational risk charge if, as you yourself noted in testimony, only "several" institutions have so far met, or plan to meet, the FFIEC's sound practices to strengthen the resilience of the financial system by year end? Put another way, why is the Federal Reserve dedicating resources to rules that would require an additional charge while many institutions and regulators have yet to use their resources to meet the desired standards?

To some extent, the development of an operational risk-based capital charge may be helping banks to better understand operational risk. However, I remain concerned that this proposed charge will only divert critical resources at a time when much remains to be done to strengthen the resilience of our financial industry. I would therefore like to be reassured that the Federal Reserve's top priority are all of the important issues detailed in your testimony. Please provide reassurance to this effect and any additional information on Federal Reserves efforts in this regard.

A. The operational resilience of depository institutions is a long-standing component of the Federal Reserve's supervisory program. The September 11 attacks served to widen the definition of risk for purposes of business continuity planning. Regulated financial institutions now are planning seriously for events that affect wide areas, have a much longer duration, or involve large loss of life or widespread destruction of property and information assets.

All depository institutions are subject to supervisory safety and soundness requirements pertaining to business continuity planning and other operational risks. These requirements have been expanded and updated over the past few years by the Federal Financial Institutions Examination Council (FFIEC). In December 2002, we issued revised guidance on information security. In April 2003, the FFIEC issued expanded guidance on business continuity planning. The guidance addresses both the operational risk and business

risk issues that depository institutions must incorporate into their business continuity plans. The guidance specifically refers to the need to plan and test for recovery of critical business functions in the event of a wide-scale disruption, as well as scenarios in which physical or information assets and personnel are lost. This year, the FFIEC issued guidance on managing additional risks arising from information technology operations, network management, and wholesale and retail payments systems. As a result, all depository institutions are becoming more resilient to today's heightened risks.

The *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (sound practices paper) amplifies these long-standing principles for a relatively small number of financial organizations that could have a systemic impact on the U.S. financial system should they suffer an operational disruption. These are organizations that provide "core" clearing and settlement services for critical financial markets--which, because all market participants rely on them and there are no substitutes for their respective functions, must meet very high standards of resilience--and a group of banks and broker-dealers that maintain at least a five percent market share in one or more critical markets. The sound practices rest on a consensus reached with financial market participants that these organizations should be able to settle open transactions within the business day on which a disruption occurs in order to assure the smooth operation of the financial system. Moreover, core clearing and settlement organizations are expected to be able to process new transactions as the markets recover. These efforts require tremendous amounts of capital investment in robust backup facilities over a multi-year implementation. Accordingly, affected depository institutions are incorporating the sound practices into their strategic plans. These expenditures will be ongoing as technology and business processes evolve.

While the capital expenditures under the sound practices paper and FFIEC guidance can be viewed as preventative (i.e., they seek to prevent wide-scale operational disruptions from having systemic effects), capital also must be maintained to account for inevitable losses that result from operational disruptions and failures. The Basel II Capital Accord

(Basel II) represents agreement by members of the Basel Committee on Banking Supervision on standards for computing appropriate levels of capital for global financial institutions. The banks that are covered by the sound practices paper are a subset of the Basel II banks. The U.S. banks that are implementing Basel II standards for credit risk also will employ the Advance Measurement Approach (AMA) for operational risk. The AMA expects that banks will use an internal assessment of operational risks to determine the amount of capital they need to support those risks. This will help assure that the banks maintain resources to compensate for unexpected losses derived from failed operations, which could include business losses as well as the cost of recovering and resuming operations, concepts that are broader than those contained in the sound practices paper. The U.S. banking agencies plan to allow considerable flexibility to banks in developing their AMA estimates, as long as their processes are comprehensive and well-reasoned. Implementation of the AMA will be evolutionary, as the relevant measurement techniques are not mature. The Federal Reserve and the other U.S. regulators believe that capital requirements cannot be regarded as a substitute for sound risk management and controls. However, the banks that are expending resources to develop internal management and measurement processes consistent with the AMA are reporting positive results in their efforts to better manage operational risks, including managing business resumption.

Governor Olson subsequently submitted the following in response to a written question received from Congressman Rubén Hinojosa in connection with the September 8, 2004, hearing before the Committee on Financial Services:

Q. Are there any particular measures that the Federal Reserve Member Banks should take to protect themselves from terrorist attacks?

A. Even before the attacks of September 11, banking organizations had instituted significant physical and cyber security measures such as perimeter and interior cameras, armed guards, security systems, protective glass, limited access to data centers and vaults, and alarm systems. Given the critical importance of information technology to the success of the banking business, banks tend to be early adopters of new technologies and have led the commercial sector in developing and implementing cyber security measures such as, for example, data encryption.

Since September 11, banks have been expected to prepare for wide-scale business disruptions that could affect the critical infrastructure of a major geographic area or cross section of the financial services industry, and for the possibility that key staff may not be available to assist in the recovery of critical operations during such disruptions. Banks are expected to incorporate into their business continuity plans measures such as increasing perimeter checks, monitoring parking areas, ensuring that a portion of critical employees are off-site for part of every business day, implementing virtual office capabilities, and developing robust, geographically diverse operation sites. Banks have shared and should continue to share best practices pertaining to the terrorist risk environment through their industry associations. The Financial Services Sector Coordinating Council (discussed in my testimony), the American Bankers Association, the Securities Industry Association, and BITS, a subsidiary of the Financial Services Roundtable, have been particularly active in this effort. The Department of Homeland Security has also issued general guidelines for responding at the various homeland security threat

levels. Banks can also work to prepare for the effects of terrorist attacks by coordinating with neighboring businesses and with state and local homeland security and protection agencies. All banks can strengthen their own resilience by complying with the Federal Financial Institution Examination Council (FFIEC) guidelines on business continuity planning.[1] Moreover, banks covered by the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, discussed in my testimony, will benefit by implementation of those additional measures, as will the whole U.S. financial system.

Over the years, banks have become increasingly reliant on information technology to perform critical functions and they have incorporated generally effective cyber security measures into their business operations. Developments in information technologies, such as the shift from mainframe computing to distributed systems and the Internet, the increased reliance on commercial off-the-shelf software, and the general expansion of potential external access to enterprise data, have increased operational risk for banks and raised privacy concerns for consumers. Accordingly, banks are expected to comply with revised FFIEC guidance on information security, which describes how a bank should protect and secure the systems and facilities that process and maintain information. The guidance calls on financial institutions and technology service providers to maintain effective security programs that are tailored to the complexity of their operations.

While experience to date shows that banking organizations are effectively managing cyber security risk, it is an ongoing battle and banks can expect to be the target of rising numbers of cyber attacks. Banks should carefully manage this risk by monitoring warnings, acting

---

[1] These and other operational risk guidelines were discussed in my testimony and can be accessed at the FFIEC website under the Information Technology Examination Handbook InfoBase at www.ffiec.gov.

quickly to apply patches in a controlled environment, and taking other steps necessary to preclude any damage to information systems. There are a number of public and private sector information sharing and analysis sites that banks can use in this process. The Financial Sector Information Sharing and Analysis Center (FS/ISAC) offers various levels of participation including a no-cost membership that provides banks and other financial institutions with urgent warning information. The FS/ISAC also now provides physical security warnings.

Other steps banks should be taking include compliance with the safety and soundness "Guidelines Establishing Standards for Safeguarding Customer Information" that went into effect in July 2001 for all financial institutions.[2] These legally enforceable guidelines require financial institutions to establish information security programs that, among other things, protect against any unanticipated threats or hazards to the security or integrity of customer records or information, and protect against unauthorized access to or use of these records or information that would result in substantial harm or inconvenience to any customer. The guidelines supplement implementation of procedures to safeguard a financial institution's information systems. The agencies have taken the position that these programs should include monitoring warnings concerning viruses, cyber attacks, software and equipment vulnerabilities, and other threats.

Finally, banks should review their internal security requirements to make sure that effective controls are in place and being followed. An important aspect of terrorist activity involves use of an insider; a significant number of hacking incidents and other attacks can be traced back to current or former employees.

---

[2] The safety and soundness guidelines can be accessed at 12 CFR 208, App. D-2, or at the Board's website under News and Events, Press Releases (January 17, 2001) at www.federalreserve.gov.

QUESTIONS OF THE HONORABLE RUBEN HINOJOSA
HOUSE FINANCIAL SERVICES COMMITTEE
"PROTECTING OUR FINANCIAL INFRASTRUCTURE: PREPARATION AND VIGILANCE"
September 8, 2004

Questions for Brian S. Tishuk, Executive Director, ChicagoFIRST

Question 2.a.

What type of regional partnerships, if any, are geared towards protecting community banks?

Answer

People across the country have important relationships with depository institutions, including community banks, savings associations, and credit unions. During and after a crisis, consumers must have access to their funds and the ability to conduct financial transactions so that they can pay bills, purchase groceries, and repair any damage to their homes and businesses.

For these reasons, community banks and other depository institutions should participate in any regional partnership available to them. ChicagoFIRST would welcome their participation and has tried recruiting them. However, they have not seen fit to pay the dues necessary to fund the organization, even though a few of our members have relatively small operations in Chicago. With our organization now well established, we plan to reach out more extensively to smaller financial institutions in 2005. Given consumers' critical reliance upon depository institutions, we have asked the Department of Homeland Security for funding to assist in this effort.

Question 2.b.

What regional partnership protects the financial infrastructure in my district, the 15th district of Texas? How can I obtain that information?

Answer

Currently, I am aware no partnerships other than ChicagoFIRST directed solely at financial institutions. Two efforts in Minnesota are open to individual depository institutions, while another group in Chicago would represent them through ChicagoFIRST. In Texas, the Federal Reserve Bank of Dallas has worked with depository institutions on homeland security issues, but I am not aware of any regional partnership.

As your questions suggest, regional partnerships should be established in several areas across the nation to enhance the resiliency of financial institutions. ChicagoFIRST agrees and has made this case at numerous homeland security conferences across the country for financial institutions. One such conference was held in Dallas in July 2003. In addition, ChicagoFIRST has worked with the United States Treasury Department and a financial trade association called BITS on a handbook that interested parties could use to establish a regional partnership like ChicagoFIRST. I can provide you with a copy of the handbook when it is completed.

ChicagoFIRST has also assisted people in other regions with an interest in forming a regional partnership. For example, I have met with an organization in Minnesota that sought advice in establishing a partnership, and I have provided guidance to those involved in similar efforts in Iowa and Ohio. I would be pleased to offer any assistance I can to those in your district with an interest in forming a regional partnership.

O