

**GOVERNMENT AND INDUSTRY EFFORTS
TO PROTECT OUR MONEY DURING
BLACKOUTS, HURRICANES, AND
OTHER DISASTERS**

HEARING
BEFORE THE
SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS
OF THE
COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTH CONGRESS
FIRST SESSION

—————
OCTOBER 20, 2003
—————

Printed for the use of the Committee on Financial Services

Serial No. 108-58



U.S. GOVERNMENT PRINTING OFFICE

92-642 PDF

WASHINGTON : 2003

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

HOUSE COMMITTEE ON FINANCIAL SERVICES

MICHAEL G. OXLEY, Ohio, *Chairman*

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

Robert U. Foster, III, *Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

SUE W. KELLY, New York, *Chair*

RON PAUL, Texas, <i>Vice Chairman</i>	LUIS V. GUTIERREZ, Illinois
STEVEN C. LATOURETTE, Ohio	JAY INSLEE, Washington
MARK GREEN, Wisconsin	DENNIS MOORE, Kansas
JOHN B. SHADEGG, Arizona	JOSEPH CROWLEY, New York
VITO FOSSELLA, New York	CAROLYN B. MALONEY, New York
JEB HENSARLING, Texas	CHARLES A. GONZALEZ, Texas
SCOTT GARRETT, New Jersey	JIM MATHESON, Utah
TIM MURPHY, Pennsylvania	STEPHEN F. LYNCH, Massachusetts
GINNY BROWN-WAITE, Florida	ARTUR DAVIS, Alabama
J. GRESHAM BARRETT, South Carolina	

CONTENTS

	Page
Hearing held on:	
October 20, 2003	1
Appendix:	
October 20, 2003	33

WITNESSES

MONDAY, OCTOBER 20, 2003

Abernathy, Hon. Wayne A., Assistant Secretary for Financial Institutions, Department of the Treasury	3
Allen, Catherine, CEO, BITS, The Financial Services Roundtable	18
Kittell, Donald D., Executive Vice President, Securities Industry Association ..	20
MacLean, Rhonda, Private Sector Coordinator, Financial Services Critical Infrastructure Protection and Homeland Security, & Director, Corporate Information Security, Bank of America	15
Olson, Hon. Mark W., Member, Board of Governors, Federal Reserve System .	5
Schmidt, Howard A., Vice President and Information Security Officer, eBay, Inc., and former Chair of the President's Critical Infrastructure Protection Board	22

APPENDIX

Prepared statements:	
Kelly, Hon. Sue W.	34
Abernathy, Hon. Wayne A.	35
Allen, Catherine	42
Kittell, Donald D.	52
MacLean, Rhonda	57
Olson, Hon. Mark W.	65
Schmidt, Howard A.	76

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Olson, Hon. Mark:	
Federal Reserve System letter, October 22, 2003	84
New York State Banking Superintendent Diana L. Taylor, prepared state- ment	86
U.S. Securities and Exchange Commission, prepared statement	92

**GOVERNMENT AND INDUSTRY EFFORTS
TO PROTECT OUR MONEY DURING
BLACKOUTS, HURRICANES, AND
OTHER DISASTERS**

Monday, October 20, 2003

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to call, at 2 p.m., in Room 2128, Rayburn House Office Building, Hon. Sue W. Kelly [chairwoman of the subcommittee] presiding.

Present: Representative Kelly.

Also Present: Representative Kanjorski.

Chairwoman KELLY. This hearing of the Subcommittee on Oversight and Investigations will come to order. This afternoon we are going to have a hearing on the government and industry efforts to protect our money during blackouts, hurricanes and other disasters. The blackout which began on Thursday afternoon, August 14, left millions of Americans in the dark in many ways. Many were stranded at work, wondering how to get home. I know many of my own constituents who work in New York City couldn't get home that night, and there were others that were stranded at airports and in other transportation systems wondering when to give up, try to find alternatives and try to get home through all the dark corridors.

In the end, major cities from New York City to Detroit were without centrally generated power. Airports, water and sewerage plants and 9/11 emergency systems were shut down. The communications systems pretty much failed. It is now even clearer that the technology age that we live in, which allows us to provide services and access information in a heartbeat, has increased our reliance on power.

It is imperative now that we review efforts to protect our systems and the infrastructure that is ever more entwined and dependent on one another. At the heart of critical infrastructure is the safety and soundness of the financial services sector. Fortunately through all of this, it appears that the financial services sector did not suffer any serious negative impacts, but we need to use the recent blackout as a test to assess the security and dependability of our financial systems. Without a doubt, there are lessons to be learned and improvements to be made.

Today we welcome Wayne Abernathy, the Assistant Secretary for Financial Institutions at the Treasury Department, who will release a special report. If you are looking for it, this is what it looks like. He is going to release a special report on the impacts of the blackout that will be crucial as to how to handle disasters in the future. Assistant Secretary Abernathy worked around the clock with many of our other witnesses who will be here today to implement backup plans during the blackout.

Joining Assistant Secretary Abernathy on our first panel is Federal Reserve Board Governor Mark Olson, who is also very instrumental in these efforts.

Keeping our financial systems functioning and safe requires a high degree of coordination between many different and important parties, both public and private. The private sector witnesses on our second panel are leaders in protecting critical financial assets from major disasters. These witnesses, along with others in the private sector and government who couldn't be represented here today, worked to ensure that our money supply and funds flow would not be jeopardized. The Depository Trust and Clearing Corporation, the New York Stock Exchange, Nasdaq, and associations such as the Bond Market Association played key roles to keep the markets working during the blackout.

Many other agencies were also involved in addition to the Treasury Department and the Federal Reserve System, including the SEC. As the regulator of the Nation's largest financial institutions, the supervisor of the New York State Banking Department, my good friend Diana Taylor, also played a key role. We thank the SEC and Ms. Taylor for their written statements which, without objection, we will submit into the record.

[The prepared statement of the Securities and Exchange Commission can be found on page 92 in the appendix.]

[The prepared statement of Diana L. Taylor can be found on page 86 in the appendix.]

Chairwoman KELLY. We really appreciate their statements. We look forward to hearing accounts of how our witnesses managed during the blackout and how emergency plans for protecting critical infrastructure, the ones that have been in place before September 11, how they worked. There is no better indicator of success of those plans than the fact that there was apparently no financial panic either during or after the blackout.

We also want to hear how prepared everyone was for a major hurricane and whether they understand what these plans are and whether or not Hurricane Isabel had any serious consequences.

I thank the witnesses for appearing here today and look forward to your testimony. Together, I hope we can ensure that our financial systems continue to function smoothly under all circumstances and the American people will continue to have confidence in the financial services sector.

The Chair notes that there will be members coming from the full committee and there will be members coming from this subcommittee. So, without objection, all members who have statements, questions to ask of the panels, and we ask the answers to those questions be included in the record. So, without objection, so ordered.

With that, I will introduce our first panel. We welcome Honorable Wayne Abernathy, Assistant Secretary for Financial Institutions at the Treasury Department, and the Honorable Mark Olson, member of the Board of Governors of the Federal Reserve System. The SEC was unable to appear today due to scheduling conflicts, so we invited the Commission to submit the statement which I have submitted for the record.

Additionally, I invited Ms. Diana Taylor, supervisor of the New York State Banking Department, to submit a statement as well about her activities in this area. So, with unanimous consent, we have entered their statements in the record.

We thank you, Mr. Abernathy and Mr. Olson, both for testifying before us and we welcome you on behalf of the committee. So, without objection, your written statements and any attachments will be made part of the record. And, without objection, we are going to continue this hearing. I would hope that you will give me a 5-minute summary of your testimony, because your testimony will—your full testimony will be in the record.

You will now be recognized for that 5-minute testimony. When the light changes color, you probably know, you have—when it goes from green to amber, you have 1 minute to pull your thoughts together and give us a summary. When it goes red, the 5 minutes is over.

Chairwoman KELLY. And we will begin with you, Mr. Abernathy. It is very—I am very pleased to have you here with us today. Go to your testimony now, please.

[The prepared statement of Hon. Sue W. Kelly can be found on page 34 in the appendix.]

STATEMENT OF HON. WAYNE A. ABERNATHY, ASSISTANT SECRETARY FOR FINANCIAL INSTITUTIONS, DEPARTMENT OF THE TREASURY

Mr. ABERNATHY. Thank you, Chairwoman Kelly, and members of the subcommittee. It is a pleasure to be here today. I am today representing not only the Department of the Treasury, but also the Financial and Banking Information Infrastructure Committee, or FBIIC. The FBIIC is charged with improving coordination and communication among financial regulators, enhancing the resilience of the financial sector and promoting communication and coordination with the private sector entities that make up and operate within our financial services sector. I represent the Department of the Treasury in chairing that committee.

Following recent events, the FBIIC conducted a review and compiled a written report that you kindly mentioned in your statement, *The Impact on the Recent Power Blackout and Hurricane Isabel on the Financial Sector*, which the FBIIC is releasing to the public today, and I submitted a copy of the report together with my statement.

Both in preparation for potential disruptions and in responding to actual threats, we are guided by four principles in order of importance:

First, and most important, we must remember in all that we do to protect our financial infrastructure, that it is always about people. It is the people that make our financial institutions work, peo-

ple that design the systems, people that make them successful, people that innovate to keep them fresh and dynamic, and it is people whom they are designed to serve; people who rely upon financial services for so many aspects of their daily lives.

Second, because it is about people, it is about confidence. Our financial institutions operate on confidence, but they also promote confidence. In fact, confidence is what our financial institutions must provide; confidence that financial transactions will be carried out, that checks will clear, that bills will be paid, that investments will be made, that insurance promises will be kept. The confidence provided by financial institutions plays a big part in helping to cope with the trauma of disaster.

Third, essential to that confidence is open markets. Financial institutions should be open for business, allowing Americans everywhere to engage in their business even during, or especially during, times of stress. It is important for financial institutions and markets to continue to operate as close to business as usual as possible.

The fourth guiding principle is that we want to promote local decision making and problem solving both as we prepare for disruptions and as we weather them. The experts that are on the ground and in the field are in the best position to determine what steps should be taken to protect employees and customers. We will help where we can, where we need to, but we intend to leave the responsibility with the financial institutions and the regulators that are closest to the problems to find the solutions. Initiative and ingenuity are the most powerful tools to deal with any disruption, and we must give full room for their exercise.

Impact of the power outage of August 14, 15, 2003. The U.S. Financial system handled the outage well. The bond market and major equities and futures markets were able to open the next day for business at their usual trading hours. Neither the Department of the Treasury nor any of our companion financial regulators received reports of lost data, significant failed transactions or other similar problems. Although there were isolated reports of telecommunications difficulties, the problems were minor and the participants resolved these problems during the day. Banks and credit unions also performed well.

Although the impact of Hurricane Isabel was less significant in degree, it was quite similar in kind to the impact of the power outage. Both resulted in widespread disruptions of electric power and the businesses that depend on it. However, the storm did not adversely affect the financial markets.

There are several reasons why the U.S. Financial system fared so well. First and foremost, the men and women who work in the financial system did an extraordinary job. During the outage many stayed at their posts to ensure that their systems preserved and processed data from trading on Thursday and that their systems would be prepared to resume trading the next day, on Friday. Almost immediately after the power went out on Thursday, financial institutions began asking themselves not whether they would open for business the next day, but how they could best serve their customers' needs. This commitment to serve customers even in times of adversity is important. I wish to note that financial institutions

decided on their own that they would open for business the next day. They did not wait for guidance from Washington.

There are many other things that we learned in terms of problems that we need to resolve. Perhaps the most important is the way in which our financial services sector depends on several others. For that reason, I would say even though the U.S. Financial system is more resilient today than it was a year ago, the men and women who work in the system help make it so and they are the ones continuing to work on the problem today.

Our job is not finished. It is a big job. To paraphrase Winston Churchill, we are not at the end or even at the beginning of the end, but we might be nearing the end of the beginning. Americans and the world can rely with increasing confidence on the U.S. Financial system. Thank you.

Chairwoman KELLY. Thank you very much, Mr. Abernathy.

[The prepared statement of Hon. Wayne A. Abernathy can be found on page 35 in the appendix.]

Chairwoman KELLY. Mr. Olson.

STATEMENT OF HON. MARK W. OLSON, GOVERNOR, FEDERAL RESERVE SYSTEM

Mr. OLSON. Thank you very much, Chairwoman Kelly. Thank you also for inviting us and thank you for holding this important hearing. My comments will be very similar to Wayne Abernathy's and very similar to the summary that you just went through with respect to the impact on the financial services industry. My focus will be from the vantage point of the Federal Reserve System and on the banking industry. And to repeat what you said, the markets remained calm and by and large and the citizens remained calm. Disruptions were relatively minor, more so I think as a result of the power outage than the hurricane, so I am going to focus a little bit more on the power outage and a little less so on the impact of the hurricane.

I think to start off, it is important to remind ourselves the fact that the disruptions were minor was not accidental. The banking industry has been faced with business disruptions over the course of its history and we had learned that business interruption is a fact of life of managing the financial services system. As a result of that, we make business continuity planning a very important part of our expectation for banking executives and we examine for the capacity and the capability of business continuity planning.

Also, I think it is important to remember that the events, first of all of Y2K and then the tragedy around September 11, 2001, has introduced elements of risk exposure with respect to business continuity that have required that we elevate the level of our preparation.

With specific focus on the power outage, as you recall, it occurred very late in the day on Thursday at about 4:11 or so, and the capital markets had closed, but very quickly the markets indicated that they would be open the following day, on Friday. As you probably know, banks are not allowed independent discretion as to whether or not to open during the normal banking day, but both the Comptroller of the Currency and many of the State bank commissioners very quickly allowed for closings should they be re-

quired. Our indication is that only perhaps a dozen banks in the entire impacted area closed, and that would be a dozen out of a universe in those States perhaps between 500 and 700 total institutions. So it was very small.

The liquidity of the markets was relatively unimpacted. The Federal funds market was impacted slightly and there was some volatility and that had to do with the fact that the Federal funds market is the interbank borrowing/lending vehicle and many of those transactions do not settle until the end of the day. So those were about to settle about the time that the power outage occurred. And so while there was volatility, it was not significantly disruptive. Also the following day, on Friday, as a result of the carryover, there was some volatility also.

From the consumers' point of view, the major impact was access to ATM machines. Some ATM machines remained open either because the branch had backup power or because the ATMs were on battery power. Consumers in general are not unused to experiencing some kind of disruptions with respect to access to ATMs. ATM machines are increasingly ubiquitous so it is not our perception that there were major problems. There are five separate Federal Reserve facilities in the area of the power outage. All of them had backup power from generators and all of them were fully functioning. As far as we know—and this is exactly what Wayne said—we are not aware of any financial records that were destroyed in the process.

With respect to Hurricane Isabel, the major advantage in preparation was that it was well anticipated. And as a result, there was more extensive advance preparation, and that was evident. And key, of course, was the communication. In terms of the agency coordination, we could see evidence of coordination on three levels almost immediately from the vantage point of the Fed. There was communication immediately among the Fed institutions and also among the agencies, the FFIEC and then more broadly among the Federal Government agencies, so the coordination was very strong.

Lessons learned: Probably the most important lesson learned from our perspective is that the best response is to be well prepared. It is a variation of a good offense is the best defense. But clearly as a result of the preparation, the anticipation of the reverse of what could go wrong helped limit the disruption.

Point number two, communications was important. And you can quantify to an extent the value of good communications. The Treasury markets for example were opened longer than the equity markets and the Treasury market dropped about 10 basis points. Long bonds dropped about 10 basis points almost immediately. As soon as the announcement was made that the outage was not as a result of a terrorist activity, the markets responded very quickly by returning to the pre-outage level. And that is a strong indication of the value of good communication. In addition to the announcement that the markets would open again on Friday these two announcements, went a long way I think in helping calm the general public.

I think another important lesson learned is the need not just for an immediate backup facility, but the ability also to provide for what might happen if that backup facility is required to stay func-

tioning for some period of time; for example, availability of a fuel source for institution using generators.

Chairwoman Kelly, we were very proud of the fact that within the Federal Reserve System a number of our employees came in on Thursday and Friday during the hurricane, many of whom stayed overnight. I would like to submit their names for the record and make it a permanent part of this hearing.

[The following information can be found on page 84 in the appendix.]

Chairwoman KELLY. So moved.

Mr. OLSON. And that concludes my opening remarks, and I would be happy to answer any questions.

[The prepared statement of Hon. Mark W. Olson can be found on page 65 in the appendix.]

Chairwoman KELLY. By all means, do submit the names of the people who did spend many hours apparently sleeping on the floor or working all night long. If you will get that to my office, we will try to see that they get some recognition and thanks for what they did. It is imperative for the U.S. economy that the markets stay open and that the banks stay open, so I am delighted to be able to acknowledge their efforts.

Thank you, Mr. Abernathy, for your testimony. I want to remind both you—both of you and the panelists for the next panel, I not only sit here on the Financial Services Committee, but I am also on the Transportation and Infrastructure Committee. And I was very interested in some of the testimony today that I was reading about the fact that there were some infrastructure problems here. I think we need to put our heads together and work to make sure it is just not the power grid going down that was the problem. From what I understand, there were issues like potable water and transportation issues with regard to getting fuel where it needed to go to keep the generators going, things like that.

I would be very interested in working with both of you and with our next panelists on addressing specifically what went wrong to see if there is something I can do to help that situation from a transportation and infrastructure decision as well. So thank you very much.

I just want to ask a few questions here of both of you. I would like to get a few details about your activities and those of the staff.

Mr. Olson, you told us your staff was there. I would like each of you to tell me where you were when the August 14 blackout occurred. I am more interested in that because it was a sudden occurrence. We had a lot of preparation. We knew the hurricane was coming, so people could prepare for it. But with a blackout, that is a sudden act and equal to something that could be akin to a terrorist act. So to me, it is very important to know how this all worked.

And I agree with you, Mr. Olson, in your statement. I believe in this instance with regard to the financial services of America, the Boy Scout motto is the best: Be prepared.

With that in mind, tell me where you both were on the afternoon of August 14, and I would like to know whether or not you were able to be in communication with the other regulators and the pri-

vate sector counterparts, what worked and what didn't work for you. If you could develop that for me, I would appreciate that.

Mr. ABERNATHY. If I may begin, Ms. Kelly, it is very fortuitous, that particular day we had chosen ahead of time as an opportunity to test one of our backup facilities and I was actually at one of the Treasury Department's backup facilities testing our ability for me to do my job from a location other than at main Treasury when this additional test occurred. And one of the aspects of the test that made it very rewarding to us was that it presented a compound question: Can we not only operate from that backup facility but can we operate in a crisis situation? And the answer is yes. I was able to do everything I could have done from my office in main Treasury at this backup facility. I was in constant communication with the other regulators. I was in regular communication with the financial services sector. I could contact the different regulators and ask them how are your markets doing, any disruptions, and I was very pleased that we are able to test both our ability to coordinate but also coordinate from an unusual site.

Chairwoman KELLY. For you, what the systems were that you had in place at that time, they worked as far as you could see?

Mr. ABERNATHY. Yes.

Chairwoman KELLY. Mr. Olson.

Mr. OLSON. It occurred late afternoon on the Thursday. And in response to your comment about the Boy Scout motto, "Be Prepared," I was fortunate that our resident Eagle Scout, Steve Malphrus, was available and he came into my office and indicated that there had been a power outage. As a result of some of the preparation that we had been through and as a result of the prioritizations that we had done previously, our first question was, are our people all right? That was the first that we have—as a result of the preparation we have done, that is—that is the first question we asked.

Second question we asked, are the Fed facilities functioning? And we determined fairly quickly that they were functioning.

I think priority number three was to focus on Fedwire. Fedwire is the large dollar payment system, and because of the fact for the most part the telecommunication system continued to work, Fedwire worked very well. We then initiated coordination with the other agencies. And as a result, we were able to learn fairly quickly that, for example, the OCC had given its pronouncement with respect to opening the following day. In terms of the priority, it was people, systems, facilities.

Chairwoman KELLY. Thank you. Each of you spent a number of years dealing with disaster planning in the financial services sector. I would like to have you grade where we stand now and how far we have come.

Let us start with how far you think we have come in terms of the grading scale. On a scale of zero to 10, with zero representing the most vulnerable and 10 representing the total fixing of the problem, the ideal, we had some vulnerabilities which may have gotten fixed over the Y2K problem, but I would be interested in your rating where we were and where we are now just on a scale of 1 to 10 to kind of give me an idea of what we need to do here.

Mr. ABERNATHY. Well, I think that presupposes a level of precision beyond where we are, but let me try to address the question this way. We certainly have been building upon preparations that have been in place over a number of years, and this is not something that the financial services sector woke up to in 2001. As you have correctly pointed out, a lot of what we rely upon today began in preparation for the Y2K phenomenon. And that built upon other efforts that had already been in place. We have financial institutions recognizing a lot of their strength comes from their reliability, and the reliability depends on the ability to operate when there is a disruption.

But each year has added to the ability to deal and cope with a new challenge. Each new challenge presents some new challenge that we didn't have before. I think what we have learned from the blackout was the more significant degree of interrelationship between the different infrastructures, as you pointed out, how communications and transportation, how water and other infrastructure tie into the ability of the financial infrastructure to operate and how they are interrelated. That is something we are probing now more than we did a few months ago, although we had been doing some of that up to that point. Probably the best I can do with regard to numbers, I would say we are much closer today to 10 than we are to zero.

Chairwoman KELLY. Mr. Olson.

Mr. OLSON. Let me just elaborate a little bit on that. First of all, I think that if you would have asked the question, for example, in 1999, the scale of 1 to 10 would have been—would have covered a limited range. Our understanding of the range of potential catastrophes is now much broader than it was then. We have a wider universe of potential issues.

Let me give you one specific example. Prior to September 11, in most of the business continuity planning that was done in the banking industry around the country, the expectation was that people would be there. Now as a result of 9/11, we recognize that we now have to plan under the assumption that perhaps the people won't be.

So I think we are still quantifying the extent to which we fully understand the risk exposures. I would say an 8 or a scale of 10 in terms of where we are now, because I think what we are doing better now than we had done before is that we have taken seriously all the planning and the need for additional testing and conducting some dry runs. I think Wayne Abernathy's experience, that he just described at Treasury, is typical of the way we are now managing that risk exposure.

Chairwoman KELLY. Thank you.

Mr. Olson, I just want to ask one question about another piece of your testimony. You said that most—there were many ATMs that were affected, but where they were located in banks and so forth, they were up and running. There are ATMs now in supermarkets, in little corner grocery stores, at a bodega, whatever. When the power went down I would have to assume that those were the ATMs that were affected, were they not?

Mr. OLSON. Probably. If they didn't have some kind of a backup power facility, either a generator or battery, those probably would

have been the ones affected. Even within the banking industry, there are some ATMs that do not have a generator backup facility or battery backup facility, but there are some kiosks, for example, where there are ATMs. So some of those might have been out also.

Chairwoman KELLY. I am wondering if it would be a function that perhaps we should consider—perhaps you should consider. We certainly don't need a law, but as you say, be prepared. We should help the public be prepared. And I am wondering if we should ask the people who own ATM machines that did not have backup power to post a notification that in the event of a blackout the ATM will not work, so that people understand that they can't in a blackout go to those machines and expect them to work. I don't know how many lives that would affect, but it seems to me we should let people know what they got, because many people do rely on a regular basis on the ATM being available, and certainly people did try to get money from ATMs in places in New York City and in my district and they were not working. I don't know what you think of that. Maybe you would like to tell me.

Mr. OLSON. I think it is an excellent question. And I would like to look into it and get back to you regarding what we have learned from that experience and the extent to which people were—the extent to which they were disadvantaged and the extent to which they were aware of alternatives and could access those alternatives. But we would be happy to follow up and get back to you on that.

Chairwoman KELLY. My concern is if it is in fine print when you sign up to get an ATM card, you are not going to notice that. But if it is printed on a sticker that is on the machine somewhere that it will not function during a blackout, that is a good thing for all of us to know. I think it is a good thing for all of us to know.

Mr. OLSON. There may be implications to that that aren't occurring to me at the moment, but we will look at that very carefully and be happy to respond.

Chairwoman KELLY. There are two other questions I would like to ask and then we will go to Mr. Kanjorski.

Mr. Abernathy, what impact did the move of the Treasury personnel to start the Homeland Security Department have on the Department's capabilities with regard to disaster planning and recovery?

Mr. ABERNATHY. As you know, Madam Chairman, we are in the process of the Homeland Security Department getting on its feet. But already in its early stages, I think one of the benefits we had was in this question of interrelating one particular sector with another, so that as we were looking at the financial services sector and finding out why certain operations continued to operate, they told us, well, we can keep going for x number of hours but we are going to run out of fuel at some particular point. We can take that question then to the Homeland Security Council and say the financial system is working well, but we may need fuel oil to be able to power generators or diesel. And so we could go to them and, say, bring that problem and they can deal with it and understand the importance of it and have in place systems to deal with that. So I think it helped in the process of connecting the different sectors together.

Chairwoman KELLY. Good. That was part of the effect that we hoped would happen.

The other thing I would be interested in hearing is have you done any—just sort of prior simulations of a blackout in any—I mean, this was not a simulated blackout on August 14, but are there simulations that you have run? Did you run one in New York City? And this is for both of you. I am interested in what magnitude, if you did run simulations, what the magnitude was and whether or not that actual blackout experience we had met what the parameters were that you had set in place if you had run those simulations.

Mr. ABERNATHY. We have participated in a number of simulations, some of which we sponsored, some of which have been sponsored by other agencies of the government. I don't recall that any of the ones that we participated in envisioned a blackout affecting 50 million people stretching from New York City to Detroit. I will say this, though, and I made the comment frequently afterwards to our staff and others as we looked at how we dealt with the crisis. We were able to deal with the problems related to the crisis not because we had practiced that particular simulation before, but because we had gone through a different number of simulation exercises, we had learned to deal with the unexpected and we learned how to communicate with one another and work through problems that we hadn't envisioned ahead of time. And that kind of exercise, the fact that we have gone through a number of different simulations, really paid off very well during the blackout.

Chairwoman KELLY. I am sure probably what you had done went a long way to keeping consumer confidence in the market.

Mr. Olson, do you want to answer that?

Mr. OLSON. I could repeat exactly what Wayne said, but let me give you an example of how it worked in the financial services industry. When the tragedy of September 11 occurred and airplanes couldn't fly and there was a tremendous amount of disruption in the economy, what we discovered, what financial institutions discovered, is they went back to the business continuity planning that they had done for Y2K and took all of the disciplines from the Y2K preparation, and those disciplines were immediately effective for them on 9/11.

And so that is a good example of how you plan for business disruption, but not necessarily for a specific one, but the planning has multiple benefits when you plan broadly.

Chairwoman KELLY. Thank you very much. I want to again—I want to hold this report and tell you I read the draft report on this and I was very, very impressed with the ability that you had in place already before that blackout to hold things together, let the markets continue to function. Of course, we were lucky because it happened at the end of the trading day in some instances; but having that report, I think, should go a long way to a certain stability and peoples' expectations with regard to anything else if we have another blackout.

I am going now to Mr. Kanjorski.

Mr. KANJORSKI. Thank you Madam Chairman.

Mr. Abernathy, you discussed the fact that the American Stock Exchange remained closed for most of the following day after the

August blackout. How will the interagency paper finalized earlier this year and in the process of being implemented by the private sector help to ensure that similar events do not occur in the future as major financial entities work to establish their backup facilities required by this guidance? What are the most important issues for them to consider with respect to electricity, telecommunications, transportation and water resources?

Mr. ABERNATHY. I think those are the key elements to look at. The purpose of the white paper—we didn't participate in the drafting of the white paper, although we are the consumers and commentators on it—that was a project of a number of the financial agencies themselves. But what we have learned from that and how it applied in the blackout is there are a number of things you can do to deal with the foreseeable, such as providing distance, providing training for personnel, making sure that you have not only facilities located in another place, making sure your backup system may not be exactly the same place as someone else's backup system is. One of the problems we discovered in 9/11, a lot of people had backup facilities, but they all had the same ones. They were sharing the same backup facilities.

So one of the things we learned through the white paper is not only ask what are your backup facilities, but how much do they overlap with someone else's. And sometimes the backup is—requires a backup to the backup, and that is a case that we have in some of the financial institutions. We have a first set of backup facilities in place, but the backup to those are now coming on-line as well, which will further reinforce our ability to switch. The other thing is make sure you have the personnel available to run these facilities.

And time, I guess, is the other factor, I would emphasize. Not only do you have the backup facility, but how quickly can it come on line. The more quickly you can bring your backup facility on line, the more quickly you can limit the damage from a disaster, and, particularly if it is a terrorist attack, the more you can take away the fruits of that terrorist attack that the terrorist is looking for. The terrorist is looking to disrupt our ability to engage in commerce. The more quickly you can bring your backup facilities on-line, you can deny that terrorist what he is trying to obtain.

Mr. KANJORSKI. Is there any task force that has the Congress's participation in the white paper or the interagency paper in terms of whether we are getting there, whether we are covering everything? As I understand the interagency paper, it states that a facility must be located beyond 50 miles of Manhattan, and I suspect that that is in order to provide for a nuclear blast. In case the city was struck by a nuclear weapon, they would want to be more than 50 miles out of the territory.

Mr. ABERNATHY. If I could make one comment, I think the 50 miles was in the original draft paper and since has been replaced with a more subjective requirement that you should have adequate distance or adequate time. The goal is you are able to get your system back up within certain time frames.

Mr. KANJORSKI. Within 2 hours.

Mr. ABERNATHY. Right. It may be that distance provides that. It may be in a financial institution you don't need the distance, you just need to have separate types of electronics or personnel.

Mr. KANJORSKI. Is somebody putting guidance together? What happens if I am handling a large part of the trades on the markets and am 10 miles away but within the blast zone? Is that considered a backup facility?

Mr. ABERNATHY. Those issues are the ones we wrestle with every day. And I would say the follow-up entity to carry out those recommendations would be the FBIIC, that on a regular basis compares notes with one another, encourages each particular financial agency to be working with their regulated entities to see how they are doing and implementing those guidelines that are put in place in the white paper; reviewing to what extent the guidelines that are in the white paper and other guidelines have become out of date due to new things we know as a result of the infrastructure as well as changing technologies.

Mr. KANJORSKI. Well, the August blackout was very informative in terms of comparing that overlay with the original thinking in the interagency paper. If you look at it and making the assumption that the 50-mile radius is the intelligent radius to be away from your major facility, then you look at what happened to electricity and find out that about half of the zone that you could relocate in, that was in the same power grid. So obviously that wouldn't be a retreat area.

And then the most significant part I think is the watershed. New York City is served with both the Hudson watershed and Delaware watershed. And in case of biological attack, it would seem to me if I were a terrorist, I would go way upstream and I would blank out a good half to two-thirds of acceptable area that backup facilities could be located in.

Is somebody testing the judgments of the companies that are making the decision to put a continuity business facility in place, or are we relying totally on their judgment to do that?

Mr. ABERNATHY. That is something in particular that Governor Olson can talk about. What we understand from the financial regulators, that kind of judgment is a constant source of discussion between the financial supervisors and the people they supervise. There is a discussion that continuously takes place in the examination process as well in the process of implementing and designing sources of resiliency.

Mr. KANJORSKI. Governor, do you want to pass on that?

Mr. OLSON. I will support what Wayne Abernathy said. As part of the supervision that we would do for financial institutions, as we would examine their business continuity planning. The FFIEC, the coordinating group, recently expanded the criteria that we use in our examination of business continuity planning from the banking industry. But you hit on the key ones. Environmental is certainly one. Infrastructure is certainly one. Availability of people is another one. And the impact, for example, of an evacuation would be another one that would be used. And since post-9/11, we have expanded the expectation.

But there are two keys. First of all, and the most important one, is people. Are you allowing for the safety of the people? And point

number two, it is the speed of recovery to get the systems back on track. So as Wayne Abernathy suggested, the idea of a specific mileage implication to it or criteria to it is less important than to be able to demonstrate the capability to respond.

Mr. KANJORSKI. One of the areas I noted in watching the various plans is the lack of adequate infrastructure for telecommunications for relocation sites. Most of these institutions have to have merit data recording, which means they have to use fiber optics and they are restricted to the speed of light, so they are restricted as to how far out they can locate from Manhattan. And I think the parameter for most of the technology companies that I have talked to is about 125 miles from Manhattan. The problem that is occurring, however, is some areas that are viable for continuity of business relocation sites do not necessarily have in place the fiber optic systems to carry the transactional load that would be required for continuity of business backup.

I guess my question to you is, are we going to do anything in the homeland security bill or appropriations to either assist utility companies or communication companies to lay that fiber optic, or is that going to be the sole burden of the companies that want to locate facilities?

Mr. ABERNATHY. I can't really respond to what is in the appropriations bill with regard to telecommunications. That is not something—

Mr. KANJORSKI. To my knowledge there is nothing.

Mr. ABERNATHY. But I would like to emphasize, though, that you are exactly right that telecommunications plays an important role on how we run our financial services. Of all the other different systems that interact with the financial services, I would probably place telecommunications right at the top. And one of the things we are engaged in and looking at very carefully is how dependent we are, and how building up redundancies in the telecommunication system can be brought forward, keeping in mind how important that is.

Mr. KANJORSKI. Even, Mr. Abernathy, getting an inventory of systems in place. Many companies refuse to disclose the locations or distances of their fiber optic systems. And it is difficult for someone to cite a continuity of business location, not knowing what the route is or the difficulty of the distance to the relocation site.

All I am raising is that there is a need for a little more comprehensive activity on the part of Treasury, the Federal Reserve, and the other regulators that are involved to make sure that we get some redundancy and we get some cooperation between other Federal and State agencies with the private sector to make sure the infrastructure is available for companies to make the proper decision as to when they can locate, where they can locate, and how quickly they can be back up in business.

Mr. ABERNATHY. I would say that interrelationship is the number one lesson we learned from the blackout, which is the interrelationship of all the different systems.

Mr. KANJORSKI. Tell me we are moving very quickly and in 18 months we are going to have all those continuity of business locations.

Mr. ABERNATHY. We are working very hard on it.

Mr. KANJORSKI. If we want to work with someone at Treasury or the Federal Reserve, who should we be talking to?

Mr. ABERNATHY. In the congressional office, John Duncan would be the person for Treasury.

Mr. OLSON. In our case, Steve Malphrus, who happens to be here, but he is the communications point.

Mr. KANJORSKI. He is the guru.

Chairwoman KELLY. Thank you. I would like to simply say that representing the area that I do, which is 50 miles north of New York City and the entire lower third of New York City's drinking systems plus major manufacturing, IBM, huge number of things in my district, we have addressed some of these things. And I think Mr. Kanjorski's question about somewhere, even if it has to be kept at an above-secret level, there ought to be some kind of an inventory, that is not a bad question. But I do know that some of this has been addressed, because I also represent the Indian Point nuclear plants and we have looked at not only evacuations but some of these other questions that had been raised.

I would hope that we can work with you both if you have needs with regard to infrastructure, so we can make sure we have what you need and we can work together.

The Chair notes that some members may have additional questions for the panel. They may wish to submit them in writing. Without objection, the hearing record will remain open for members to submit questions and place responses in the record.

This panel is excused with the committee's great appreciation for your time. Thank you very much.

I would like to introduce our next panel. First is Ms. Rhonda MacLean, Private Sector Coordinator, Financial Services Critical Infrastructure Protection and Homeland Security issues, and the Director of Corporate Information Security at the Bank of America; Ms. Catherine Allen, CEO of BITS, at the Financial Services Roundtable; Mr. Donald Kittell—hope I pronounced that right—Executive Vice President of the Securities Industry Association; and Mr. Howard Schmidt, Vice President and Information Security Officer at eBay, and the former Chair of the President's Critical Infrastructure Protection Board. We thank you all.

Chairwoman KELLY. And we will begin with you, Ms. MacLean.

STATEMENT OF RHONDA MACLEAN, PRIVATE SECTOR COORDINATOR, FINANCIAL SERVICES CRITICAL INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY, AND DIRECTOR, CORPORATE INFORMATION SECURITY, BANK OF AMERICA

Ms. MACLEAN. Thank you, Chairwoman Kelly and Representative Kanjorski, as well as members of the subcommittee for inviting me here today for this important hearing. I am honored to be here to speak on behalf of the financial services sector and my role as the Department of Treasury-appointed Private Sector Coordinator for Critical Infrastructure Protection. The financial sector chose to form a Financial Services Sector Coordinating Council with the public sector support and encouragement and with Treasury's leadership.

I want to recognize Treasury Assistant Secretary Wayne Abernathy and Deputy Assistant Secretary Michael Dawson for their instrumental leadership in promoting and supporting our efforts for an effective public-private partnership. It has really served as a model for other sectors such as telecommunications and energy and the like. The council consists of 25 organizations that through their constituents represent the majority of the financial services sector. These organizations include key national exchanges; clearing organizations; trade associations in the banking, securities, bond, and insurance segments of our industry; and key professional institutes.

Information provided in my written testimony identifies the members of our council and additionally includes a diagram depicting an extremely important aspect of why we believe our sector has such an effective and real public-private partnership at the sector level.

As Mr. Abernathy indicated, the public sector has formed the Financial and Banking Information Infrastructure Committee, the FBIIC. And periodically both members of our council and the committee need to discuss and work together to address sector-wide issues and initiatives that focus on strengthening the resiliency of our sector.

Our councils work on five strategic areas and I will briefly discuss each of those:

First is the information and dissemination and information sharing. Our goal here is to provide a universal service for disseminating trusted and timely alert and warning information to all sector participants. We believe that this type of information sharing will continue to increase the general overall knowledge about physical and cybersecurity operational risks that face our sector. We have gone from approximately 70 financial institutions receiving this important information to now over 8,000 who are receiving this information today. This significant step forward in our goal was accomplished through the many council members leveraging their constituents' contacts to distribute the critical alerts. Our next generation ISAC will continue to improve on this information dissemination directly to the financial institutions themselves. The sector awareness and outreach activities we are implementing is a program for homeland security and information—critical infrastructure protection initiatives that include regional forums. The local and regional efforts are in most cases the front lines in the times of crisis and are an important element in the overall communications flow during the times of crisis coordination and crisis management. The council also has a research and development task group that is working with Treasury to determine priority for research and development needs of our sector. We have also been working on our Sector National Strategy to revise that document in response to the two national strategies President Bush released in February. This is our vehicle to really define tactical, actionable and measurable programming to direct and advance our sector-wide critical infrastructure and homeland security efforts for the resiliency of our sector.

Lastly, the subject of this hearing has focused on the council's efforts around crisis and response management. When events occur

with broad sector or national impact, a plan and adopted approach for sector-wide crisis management must exist, including coordination with government entities and other critical infrastructure sectors on which we depend. At a sector level the council uses a crisis communicator capability developed and supported by BITS that allows council members to convene in times of emergency. Timely communication and effective coordination is essential to ensure the financial sector maintains its resiliency and ensures public confidence. We have had numerous opportunities to trust our crisis management procedures at a local, regional, and sector level. If we examine the August blackout, which had larger geographic impact than Hurricane Isabel from a power outage perspective, we came through those events beautifully but also with the lessons learned as described before.

As sector coordinator I was able to participate and receive information from numerous activities led by council associations, clearing corporations, and Treasury-led government teams. Additionally, because of the close working relationship developed among sector coordinators while working together on critical infrastructure protection initiatives, our sector received regular updates on restoration activities. In the case of the blackout, Mr. Michael Gant, sector coordinator for the electric power, provided regular updates and outage progress and really worked with us in our coordination effort. This level of direct communication was invaluable as efforts occurred to evaluate the situation and plan next steps.

This past Thursday and Friday our council held its regular quarterly meeting in New York City where lessons learned were discussed by the council and FBIIC with the New York Office of Emergency Management. It was clear that the blackout allowed many organizations to apply crisis communication and management improvements post-9/11. The council members decided to work on identifying the various calls that now typically occur in times of crisis and will use the blackout experience as a case study. The sector-wide effort being undertaken by the council will seek to identify opportunities for improving sequencing of these calls and other options for better information flow and emergency communications. This effort will be coordinated with our public sector colleagues and other sectors upon which we have specific dependence.

My two colleagues on this panel, whose leadership for our sector has been instrumental in the formation of the council and leadership within the council, will be speaking on some of the outstanding work their organizations have accomplished and specific lessons learned from both the blackout and Hurricane Isabel, together with recommendations.

Ms. MACLEAN. In summary, Chairwoman Kelly and members of the committee, we believe that a strong public/private sector partnership is the primary reason for our success. The Government and the private sector's coordinating efforts during the recent power outage and storms demonstrated the preparedness work done by many organizations that have yielded very positive results. These efforts have helped to ensure our critical efforts are resilient and we are worthy of maintaining the public confidence.

Thank you for your opportunity to testify.

[The prepared statement of Rhonda MacLean can be found on page 57 in the appendix.]

Chairwoman KELLY. Thank you, Ms. MacLean.
Ms. Allen.

**STATEMENT OF CATHERINE ALLEN, CEO, BITS, THE
FINANCIAL SERVICES ROUNDTABLE**

Ms. ALLEN. Thank you, Chairwoman Kelly and Congressman

Kanjorski and other members of the committee, for the opportunity to testify. I am Catherine Allen, CEO of BITS, a not-for-profit industry consortium of the 100 largest financial institutions in the U.S. BITS is the sister organization to The Financial Services Roundtable, and our mission is to serve the financial services industry where it interfaces between commerce, technology and financial services. We are not a lobbying organization.

Our work is shared not only among our members but throughout the financial services sector, and you will see that in a minute. I experienced firsthand the outage. We were in Detroit at BITS meetings and experienced not having water, power, telephone and many of the other things, along with the CIOs and CTOs of a number of the financial institutions.

Bottom line, the financial services industry and our customers fared well. Backup systems worked, ultimate communications systems were used, and there was no measurable impact on settlement and payments. There was excellent cooperation in communications among the financial services regulators, Treasury and the financial sectors.

Three major reasons why I think the Nation's system fared so well were, first of all, preparation. As Mr. Olson said, the events of 9/11 and subsequent preparations by both the private and public sector helped us trust each other and helped us with our abilities to communicate, shift to backup systems and continue operations.

A second thing was the early announcement that this was not a terrorist event, and I cannot reinforce how important that was. This helped to alleviate public concerns and made for orderly execution of business continuity processes.

Thirdly was the diversity of communications. Again I personally can attest to how you use cell phones until they run out of juice and then you use Blackberrys and you save cell phones to communicate with others. Actually, throughout the event Assistant Secretary Wayne Abernathy and I were Blackberrying back and forth in preparation that BITS and the Roundtable held.

There also were some critical lessons from the event. The power grid must and should be considered among the most vital critical infrastructures that needs investment to make sure it works. The cascading impact cannot be overstated.

Secondly, water for cooling systems and personal hygiene is often controlled by electricity. People do not think about that, and that is what caused many organizations to close their offices or delay opening.

Lastly, communications must be viewed as an integrated system. We must be able to use diverse communications and understand the vulnerabilities, address those vulnerabilities and make sure we have diversity and redundancy.

Attached to our testimony is a wide variety of lessons learned from the outage and specific recommendations. We gathered these from what our members experienced during the outage.

The most important lesson, however, that was learned was how interdependent the critical infrastructures were and also how fortunate we were that it was not a terrorist driven event or we had a cyber security event at the same time. We need to look strategically and holistically at the Nation's critical infrastructures and what can be done to enhance resiliency, reliability, redundancy and diversity.

BITS has addressed a number of the interdependency issues and Congressman Kanjorski, you are right on about your points about the telecommunications industry. That has been our most important effort this past year, the understanding of the inventory and what they had and how we would know whether they had backup offices.

BITS has led an effort on behalf of the financial sector in assessing telecommunications vulnerabilities and enhancing recovery. We have worked with the National Communication System, the NCS, of the DHS, who are helping us, and I can say there is unparalleled cooperation going on right now between the telecom and financial sectors. The results have included a detailed and confidential assessment of the interdependencies in these routes that you were mentioning in a specific geographic area and we are looking at how we replicate that through other areas.

Best practices in telecommunications and financial procurement policies, pilots to model the costs of attaining greater diversity and redundancy, adoption by our CEOs of the NRICK best practices in physical and cyber security and obviously education in both sectors. There are many other things that we have done in the crisis management area.

I will point out two areas that also relate to this, and that is the IT service providers. There is a press release accompanying this hearing that talks about the BITS framework for managing technology risk. We must look at our IT service providers and our vendors as closely as we look at ourselves and we have to make sure that we manage the risk—our risk management strategies are in place in working with them.

Secondly is the area of software security. We have worked on a BITS product certification program where we test software products against security criteria the industry developed.

Again a press release accompanies this hearing, talking about the development of a user driven coalition to address the issues of software development, as well as the patch management process. We urge the committee to consider all aspects of critical infrastructure, the software and operating systems, the service providers, the critical infrastructure industries and the practices of firms, industries and Government in addressing not only these power outages but future disasters and related events.

I will end with the five key recommendations that we have with the committee. One is to invest in the power grid because of its critical and cascading impact; in fact, investment in a number of the critical infrastructures, such as power, telecommunications,

and transportation, their incentives, such as tax credits, credits for investment, R&D investment and direct Government investment.

Number two, announce early whether an event is terrorist related, or not. I cannot tell you how critical this was to our maintenance of our crisis management procedures and communications.

Three, establish improved coordination committee procedures across the critical infrastructures, specifically with the Federal, State and local government.

Number four, recognize that the financial sector is driven by its trusted reputation as well as regulatory requirements. Not all other sectors are the same way, and we need to look at this again holistically.

And lastly and most importantly, recognize and review the dependence of all critical infrastructures on software operating systems and the Internet. A cyber attack of some kind which impacts communications, SCADA systems and first responder systems would put us at terrible risk. Compounding the problem is the lack of security software development processes and a current inefficient software patch process that not only cost us millions but put us at greater risk.

It is an alarming issue and critical to the Nation's infrastructure. A clear understanding of the role of software operating systems and the higher duty of care, particularly when serving the Nation's critical infrastructures needs to be explored.

Again, thank you for this opportunity, and I will look forward to answering questions.

[The prepared statement of Catherine Allen can be found on page 42 in the appendix.]

Chairwoman Kelly. Thank you very much.

Mr. Kittell, please.

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

Mr. KITTELL. Thank you, Chairwoman Kelly and Congressman Kanjorski.

I am Donald Kittell, Executive Vice President of the Securities Industry Association.

Since 9/11 the security industry has invested a great deal of time and resources in business continuity plans. The opening of the market following the blackout I think was clear proof that those plans were viable, at least in the event of a blackout occurring at about 4:30 on a Thursday afternoon. I would particularly highlight the support we received from New York City, as well as from State, Federal and regulatory bodies during the event.

Early assurances that this was not a terrorist act was very important, and after 9/11, dealing with the blackout was a refreshingly easy problem. When street power was lost, there was essentially a seamless transition to backup power among all the firms and the exchanges. The Securities Industry Automation Corporation, or SIAC, processes for the New York Stock Exchange, the American Stock Exchange, the National Market Systems, Depository Trust, Fixed Income Clearing and other organizations. Those sites were protected by battery backup combined with backup gen-

erators, and there were no interruptions in processing and no loss of data.

Similarly, SIAC's safety system, which was installed subsequent to 9/11 to provide alternative telecommunications connectivity between securities firms and the infrastructure exchanges, operated throughout the blackout without difficulty.

Depository Trust activated both its remote sites and its remote operating locations, both of which were developed following 9/11, so they were actually operating their data center in New York from a remote operating center successfully.

The American Stock Exchange, we talked about earlier, was able to activate backup generators for its building and trade systems but not its cooling systems because of a shutdown of ConEd steam power. The AmEx obtained emergency steam generation power later on Friday, was able to open and perform an orderly close at the end of the day.

But I would like to come back to Congressman Kanjorski's question about the AmEx if we have time later.

Some securities firms relocated to backup sites, others operated under both backup and main primary sites, but essentially all firms were able to operate following the blackout.

SIA's command center was activated within minutes of the blackout and conducted conference calls throughout Thursday night, the following Friday, and into the weekend, and these calls were integrated with those of the regulators and other industry organizations.

SIA has maintained a seat at the New York City Office of Emergency Management since the Y2K days, and that was invaluable; in fact, it was the OEM that arranged the backup steam for the AmEx, as well as arranging for delivery of fuel to backup generator sites.

We believe there is value to adding other people to our network of calls, primarily in the telecommunications area, but also with data vendors and service bureaus, and we are working to accomplish this. I think the main thing we have learned with these calls is that it is not so much the preparation and structuring of them but just the flexibility we have of being able to talk to each other when an event occurs.

There were some infrastructure issues. The two worst problems were loss of communications and transportation. The cell phone service degraded pretty rapidly once the backup battery power was over and some of the land line switches in Brooklyn and mid-town Manhattan were disabled. Instances were identified where fuel delivery trucks could not be reloaded because of, again, pumps that did not have backup power.

Transportation systems were immobilized, and many employees were stranded. Actually, this was a good thing from the standpoint of opening the markets but not so good for the people involved. Ferries continued to operate but they were overwhelmed by the number of riders. As a result, many firms are reconsidering plans to keep critical employees on-site as well as shutting down their operations and sending people home.

Vis-a-vis Hurricane Isabel, the New York City OEM was our primary source of information, and fortunately we were able to avoid

any major challenge there, but we are very cognizant of the risk we run in Lower Manhattan of a hurricane. We were fortunate that both the blackout occurred when it did and that the hurricane did not impact New York in a significant way.

The blackout occurred after trading hours in daylight, on a Thursday of the week. It is just about the best time we could order up a blackout. We would have faced very significant challenges if it had occurred during trading hours or if it had occurred early in the morning before the work force actually was able to get into the city.

With respect to the hurricane, we are well-aware of the potential flood damage in downtown Manhattan. Again, New York City OEM would be our key guidance there as far as evacuation is concerned, so although the early reports and preparation were fine, I think we are very cognizant of the fact that a hurricane with a direct hit in New York would present much more serious problems than what we had with the blackout.

Since 9/11, the industry, in partnership with Federal, State and city emergency management associations, regulatory agencies, service providers, has improved its resiliency. We are proud of the progress to date. We continue to address vulnerabilities in the future.

Thank you, Congresswoman Kelly.

[The prepared statement of Donald D. Kittell can be found on page 52 in the appendix.]

Chairwoman KELLY. Thank you very much.

Now, we turn to you, Mr. Schmidt.

STATEMENT OF HOWARD A. SCHMIDT, VICE PRESIDENT AND INFORMATION SECURITY OFFICER, eBAY, INC., AND FORMER CHAIR OF THE PRESIDENT'S CRITICAL INFRASTRUCTURE PROTECTION BOARD

Mr. SCHMIDT. Thank you very much, Chairwoman Kelly members of the committee. My name is Howard Schmidt. I am the Vice President and Chief Information Security Officer for eBay, where I lead a team who is responsible for the security, trustworthiness and availability of the services that bring so many global citizens together each day.

Today I come to you more as an individual, primarily, who has had the privilege of working with many committed individuals in the private sector, law enforcement and government to forge a collaboration and cooperation to essentially safeguard the sort of resources we need through cyberspace and we have seen protected as a result of the blackout.

I had the privilege of assisting in the formation of some of the first collaborative efforts in this arena and led the creation of the Information Technology Information Sharing and Analysis Center, or the IT-ISAC, and now I am serving as the first President. This was in the aftermath of PDD-63.

Later I was appointed by President Bush to serve with Richard Clarke running the President's Critical Infrastructure Protection Board, in which many of the issues we are talking about here today were part of the key issues we were looking at as we put together the National Strategy to Defend Cyberspace, and that national

strategy, I might add, was a combination of work done by BITS, the Financial Services ISAC, many of the Federal Government agencies, as well as the Congress and many of the private citizens across the United States.

But I want to talk for a moment about the successes that the financial services community had that enabled us to continue business during the blackout and the recent hurricane. It served to deepen our appreciation of the interdependencies between the Internet and the critical infrastructure and those pieces of commerce that we depend on, as many saw the perfect storm of the convergence of two Internet worms that were occurring at the same time the blackout was taking place, but also, as the Congressman pointed out, between the power and telecommunications infrastructure. We were also reminded that much of the work that we did in the preparation of the cyber security plan also gave us the resiliency and the ability to protect ourselves because those same plans in a cyber attack were the same plans we needed to put in place to minimize the effect of the blackout we saw.

One of the things that has helped reduce the impact of this event as well as others is the ability to share information across sectors and across competitor lines. It was particularly rewarding to see many companies, strong competitors in the marketplace, share information about backup strategies, share information about disaster recovery sites. So we can indeed enjoy the benefits of the services they provide us on a day-to-day basis.

As a matter of fact, during the summer events for the blackout, we saw for the on-line industry approximately a 10 to 15 percent reduction of activity during the power outage itself, but that was primarily related to the fact that many citizens who would use the Internet could not even log on to be able to conduct some of the transactions, but in doing so, one of the resources we turned to was the financial impact report by various industries, and looking at this, it cited in the report the credit card and sales authorizations, which is one of the main focuses we looked at with eBay, for online sales would lose \$2.6 million an hour if they were unable to conduct their transactions, and even home shopping was estimated to have losses of \$113,000 per hour if the system was not available.

There is much we can do to prepare for these sort of events, and once again I cite the interrelationship between cyber attacks on our infrastructure or the critical events we have seen this summer.

In this case, the Internet connects about 170 million computers and an estimated 680 million users. There is an estimated growth rate going to 904 million by the end of 2004, and you can see eBay is a prime example of how deeply ingrained the Internet is to American life and the dependency we have on the power of the telecommunications systems to bring these buyers and sellers together.

More fundamentally, and I think this is pretty important to understand this, by our location in the backup strategies and the redundancy that we have in the overall infrastructure system, the stores stayed open during the crisis times where physical stores were incapable of opening at that point.

I want to also point out that some of the emerging solutions we have are some of the issues around the United States Computer

Emergency Response Team, which has just now been appointed up in Carnegie Mellon University by the Department of Homeland Security.

By bringing the sector coordinators such as Rhonda MacLean, the Information Sharing Analysis Centers, by participation of many of those folks and the work done in PDD-63 with the Department of Treasury, Department of Homeland Security, we can then continue to move forward and make sure that those disruptions we have seen indeed have minimal impact on our ability to transact business online and particularly in the financial sector.

In closing, I just want to comment on the fact that one of the, I think, keystone milestones that we are seeing coming forth is in the first part of December the Department of Homeland Security, in conjunction with many of the folks that you have heard from my colleagues here today are putting on a National Cyber Security Summit out on the West Coast, and this summit will be cohosted by private sector organizations, the Department of Homeland Security, Department of Treasury, and we intend to as a result of that put together a task force which will continue to evolve in a position where the power blackouts, the effects of the hurricane will have less of an effect on the infrastructure we depend on, both telecommunications and the power blackout, and we will continue to work on these plans going forward and working with your committee to make sure that we serve the American public as well as the private sector interests of the country, with which we are both very much in tune.

Chairwoman Kelly, this concludes my remarks and I welcome any questions that you have.

[The prepared statement of Howard A. Schmidt can be found on page 76 in the appendix.]

Chairwoman KELLY. Thank you very much, Mr. Schmidt.

Can you tell us the date of that?

You just said that you are going to have the Cyber Security Summit, but you didn't, I believe, mention the date. Even if you did, let's emphasize it.

Mr. SCHMIDT. I did not. It is in my written testimony. It is December 3rd, and the venue is still being worked on by DHS, and I understand Secretary Ridge is also having a personal hand in putting this very, very valuable summit together.

Chairwoman KELLY. Yes, I am sure it will be valuable.

We have been talking about a number of problems with IT software, as well as the hardware, and I am hopeful that both of those will be addressed at that summit?

Mr. SCHMIDT. Yes. As a matter of fact, they are. There are two specific task forces looking at quality control and engineering, and taking the efforts that many of the software companies and hardware companies have really turned their business models around to focus on security and availability; as a matter of fact, to the displacement of some of the feature issues that we are going to have a complete task force work with those issues to make sure that that gets accelerated.

Chairwoman KELLY. Given your White House background, I would like to know how the financial sector would have handled the power outage in August differently had it been the result of a

terrorist attack or if it had been a particular terrorist attack on a cyber section.

Mr. SCHMIDT. I think that is one of the interesting points, as I tried to point out during my testimony, that many of the resources and many of the programs that we put in place relative to the aftermath of September 11 and actually going back even to PDD-63 were the same things we needed to do for disaster recovery of business continuity, so therefore had we not had the focus we had over the past 5 years I think it would have been a different story. So whether it is a terrorist attack, a cyber attack, I think the steps the financial sector took in preparation of this are the right steps and they continue to move in the direction to even make this more valuable.

Chairwoman KELLY. Thank you.

I would like to ask Ms. MacLean, what was, for your group and for you possibly and your sector, what was the biggest surprise that you found during the blackout, a problem or something that worked that you didn't think was going to work?

Ms. MACLEAN. I think the biggest—well, it was no surprise that it worked, and that only came because of the amount of testing and focus this particular area, business continuity and resiliency, has on our sector in general.

I think the biggest surprise for me was in actually setting on some of the telecoms the issue of dealing with some of the personal inconveniences for people, such as the sanitation systems being dependent on the electric power, and I know in our case and some of the New York buildings being on a very tall floor was a very inconvenient process, and so making sure that we had good sanitary conditions, together with getting food in to people who had stayed through the night and through the days following the blackout, to make sure everything was operational I think was the key thing that—and also making sure we had enough flashlights, because that is another area where you may have backup resiliency but you really do not have enough to power lighting, and so you need to have other kinds of capabilities there on hand.

So it is the people issue again that I think continues to have additional focus in many of our institutions.

Chairwoman KELLY. What do you think should be done with regard to battery backup? I understand that there were places that had battery backup but then after a while the battery simply expired.

Ms. MACLEAN. Well, for the systems to maintain operational—I mean, that runs on large generators, that provided adequate backup. I think the smaller battery backup just for a small area I think is where it gets a little bit more complicated and I think we need to look at what are some of the alternatives. Again, I think it is more of a people issue rather than it is the system. The systems are going to be run through the large generators, which seemed to have adequacy.

Chairwoman KELLY. I am interested in the mix that we have been talking about, this interrelationship, and you pointed out sanitary systems on the upper floors weren't exactly working, and Mr. Kanjorski brought up the fact that there were some problems that

possibly could have been some problems with regard to drinking water.

Your sector—or any of you, let me address this to all of you: Are you planning to try to work with the third parties that control these systems to try to put something in place fairly soon or do you feel that is just the way it is going to be?

Ms. MACLEAN. Well, let me take a cut at that answer. I think the sector coordinators, there is a sector coordinator for water and power, for emergency, I mentioned Mr. Michael Gant. There is also a telecommunications sector coordinator, and we do meet on a regular basis and this is the focus of a lot of our talk in discussions and looking at what are the initiatives we need to have cross-sector to make sure that we are working together.

The interdependencies is what is at—is the main point that we need to get at, and I understand those intersections of interdependencies, and make sure we have adequate plans in place to address those things.

Mr. KITTELL. Our best work there is with the New York City Office of Emergency Management, where we get more results with the OEM talking to the water companies than we do talking with the water companies directly. Same thing with telecom in an event like this. So that problem is identified on our list of things that we are chasing down.

Chairwoman KELLY. That is good to hear. I suspect we in the New York area have had—obviously, we have had a little more experience in some other areas in dealing with this, but I just still do not think we have it put together. I think it is very important that these integrations of systems be worked on and be made to work.

I have other questions. I will submit some of them in writing, but in the interest of time I am going to go to Mr. Kanjorski.

Mr. KANJORSKI. I thank Ms. Kelly.

Ms. MacLean and Mr. Kittell, one of the most important aspects of disaster recovery planning for very large financial entities and for clearinghouses concerns the maintenance of a synchronized realtime redundancy.

As I understand, to address this issue many firms currently rely on annual descriptions to the disaster recovery systems, be it known as SunGard and IBM Global Services, but when a disaster strikes at these first, first in line in receiving assistance, they may not be first to receive help.

What will happen to our markets if all of the disaster space is taken? What could financial firms do to prepare for such contingencies?

Mr. KITTELL. Well, I think we had that situation with 9/11, Congressman. The backup sites at the companies you mentioned were swamped with all of the firms that were affected by 9/11 and they did, I would say, a very good job of not only using their preplanned space but also giving up their own offices and data centers for use by the firms that needed it.

There was also a tremendous—as you know, there was a tremendous voluntary effort on the part of other firms in the industry, offering desk space and data center space, and so on, in a cooperative way across the industry, so I think we have already had that event.

I think as a result of the event the capacity in those backup organizations has been increased, and, you know, depending on the nature of the event to come, we are certainly in much better shape than we were pre-9/11. Whether we could defend against some of the scenarios that people talk about is obviously an open question.

Mr. KANJORSKI. Do you want to respond along that line?

Ms. MACLEAN. Well, I think Don Kittell has really done a good job of articulating. The 9/11 really did—at the end of the day, we did work very, very well, even though we did reach capacity. As a result, though, also, you mentioned the interagency white paper that has been published. Institutions are required to look at those recommendations in that white paper and are in the process of implementing and assessing their programs against that, the recommendations made in the interagency white paper.

As we go forward, the focus is really to continuously improve and assess your capabilities and ensure that you can meet those 2 and 4-hour guidelines, and I think that is where the real question comes in, is the innovativeness and the different capabilities that we can bring to bear to meet those time lines, and that is where the focus is today.

Ms. ALLEN. Yes, I might just address that, too, because we have done work in the outsourcer area, we have viewed them as third parties, and that is part of what this framework that we developed for the industry was, to look at present best practices that financial institutions need to require of their third-party providers.

We actually are having a meeting on this, a conference on this, on outsourcing, on November 6 and 7, and, again, it focused on preparedness, on the requirements, so that outsourcers meet the same level of standards that we require internally and to look at where the gaps are, so that we make sure that we have enough capacity in the outsourcing industry to handle it if we have a major disaster.

Mr. KANJORSKI. Does that create some unfair competition, if some companies respond by doing the job in accordance with the white paper and others decide to take the chance not to do it? If a disaster doesn't occur, the latter group gets a competitive advantage. Of course, if the disaster does occur, the former group gets a competitive advantage. And if someone looked at whether or not there was a need for compulsion as opposed to voluntarism?

Ms. ALLEN. That is my point. The point about the financial institutions were all regulated. We all have certain levels of regulation or compliance that we must meet, but we oftentimes compete with nonfinancial institutions who do not have to meet the same regulatory oversight or liability or business compliance requirements that we do, and it is one of our reasons we focus on outsourcers, to make them meet the same requirements, but they aren't really regulated. It is only at our request or our demands that they meet that.

Other critical infrastructure facilities that we rely on, we totally rely on in some cases, do not have the same regulatory oversight or do not have the same kind of requirements that we do. So that makes it difficult. The interagency white paper is a good example of requiring us to come back up in a certain time period. We can do what we can internal to our walls, but when we are dependent

upon the telecommunications or the power industry, we cannot always be sure that they will be there.

Mr. KITTELL. I would comment on that. I do not think firms look at this as a competitive issue the degree to which they build resilient facilities.

The issue that is debated is what events do you defend against and which ones have a high enough probability that will result in the investment paying off, and that is the debate that takes place between firms individually and with the regulators, whether it is the Fed or the SEC or the Treasury.

What events have I agreed to defend against and how have I defended against them, and there are some scenarios that some firms freely admit they are not pretending to defend against, but I think that is the primary debate. What do you defend against and what do you not? It is not a question of competitiveness, one way or the other.

Mr. KANJORSKI. Thank you very much, Ms. Kelly.

Chairwoman KELLY. Thank you.

Ms. Allen, I would like to go back and ask you a question about the outsourcing problem that you raised.

We talk about cost/benefit, and my next question is going to be to this panel on cost about all of this, but one of the reasons we see an increase in outsourcing in a number of areas is it does cost less.

From what you now know, do you believe that there is a Federal regulatory position that we should be thinking about taking, with regard to people who do affect our financial structures who are in an outsourced position and perhaps not on the shores of the United States of America?

Ms. ALLEN. I would have to come back with an answer on whether you should take a regulatory perspective. I will say that that is a target. The idea of having industry marks and best practices and requirements of outsources, whether they are inside our territory or whether they are in India, China, or other places, our financial institutions are requiring the same level of standards of those two types of outsourcing entities, and I think that it is important that a number of the regulators will go into major outsourcers, providers that provide the majority of services to the financial institutions and actually will examine them. It is on a limited basis, but it also is helpful in making sure those outsourcers know they are going to be looked at in terms of their capabilities.

I would have to come back to you on the regulatory part of it.

Chairwoman KELLY. When you said that you require the same level of standards, we have been talking about the fact that we here in the United States, while we do have a lot of standards, some of our standards were deeply affected by the availability of power, water, and so forth.

Are those levels required of outsourced?

Ms. ALLEN. Again, we are asking in the framework, and we also are ready to launch a major, what I call, security assessment, it is a matrix. It is standardized, whether it is a financial institution or a consultant or auditing firm goes in and looks at an outsourcer, it is the same questions, again whether they are located in the U.S. Or outside the U.S., their dependency on power, on telecommuni-

cations, having backup systems, making sure they can get people to their sites. So we are viewing them just the same as having our own backup system 50 miles away or 200 miles away. If it is 2,000 or 20 miles away, it is the same way looking at that outsource capability.

Chairwoman KELLY. Thank you very much.

I want to go back and ask you all the same question: Has there been a study, do you have any idea what the cost is, with regard to planning, putting in place the things that we need to make sure that the systems, the financial systems in America stay up and running despite any kind of a disaster?

All of the disaster planning we have done has cost money. Your conferences cost money, and this money is currently coming from the private sector, so we in the Government really, I do not think, have a handle on it.

Do any of you have a handle on it and can you tell us what the costs look like, and I am going to start with you, Ms. MacLean.

Ms. MACLEAN. Well, there has been a number of different studies that you can—the Gardiner Group I know has done some marking between different institutions where you can get some comparison data about what the investment is with large organizations or medium organizations who are looking at their business continuity and business preparedness. So there is some independent individual studies for the purpose of marking.

I am not aware, maybe some of my colleagues here are aware, of an overall study that quotes would be a good source of something, but that is something we surely could look into and make available to you and to your staff.

Chairwoman KELLY. I am just wondering about the insurance industry. For instance, they said that the cost of the blackout could be estimated in several billion dollars from what I understand.

I want to know if there has been any objective look at the losses in that sector alone, let alone all the things we have put together. So perhaps we could take a look at that.

Ms. ALLEN, would you like to respond to that?

Ms. ALLEN. There are isolated studies, again the Gardiner study, we ourselves are dimensioning the costs to our industry of patch management, what it costs to go back in for the Slammer, for the SoBig to fix that, so we have a handle on how big this issue is.

We could come back to you, and I will give you some isolated studies that I have seen on the cost of business continuity, cost of requirements to be able to have the kind of physical security you need.

We are working with the telecommunications industry right now to dimension the cost to provide the level of diversity and redundancy that they now provide to the FAA and if we were to provide that to financial institutions. There aren't numbers on that yet, but we will be happy to share that once we know it.

Chairwoman KELLY. Mr. Kittell?

Mr. KITTELL. Yes.

The SIA did a cost study of the Y2K conversion at something in the neighborhood of \$5 billion over 3 years. We did a similar kind of study for the conversion of decimals, which was about two billion over 2 years, or so.

We also did a cost estimate of moving from T3 settlement to T1 settlement, of about \$8 billion over about a 4 or 5-year period.

These numbers are very gross. They will take into account IT and other budgets that are addressing lots of other things besides the specific projects that we talked about, because they get into fundamental infrastructure capacity.

It is very hard to isolate one number from another. We have not done a number on business continuity planning over the last 2 or 3 years, but depending on who is calculating and what objective they are trying to reach, I would say you would see numbers comparable to maybe the decimal conversion or Y2K.

Chairwoman KELLY. Thank you.

Mr. Schmidt.

Mr. SCHMIDT. Yeah, I do not know of a comprehensive study, but some of the university relationships I have had, I am going to go back and ask them to start working on one and ask them to prepare for that. But this Eagle Rock Alliance out of New Jersey has done an hourly breakdown on what the losses might be, and I found that particularly interesting on some of the data points they have got, but the whole issue of the availability, part of the service level agreements that many of us are now doing—and I believe Catherine mentioned it—with our outsourcing partners, that basically we are not only having that as part of the contractual agreement but we are also engaging with other companies to do an audit to make sure they can deliver on that. So it is having a cascading effect on some of the smaller partners out there, which then gives us a better availability later on to say yes, we can deliver within that 2 to 4-hour time frame.

Chairwoman KELLY. Thank you. Would this panel have any final recommendations for this committee with regard to the issue we are addressing today?

Ms. ALLEN. I would just like to commend Congress for passing the Defense Production Act with the definition of critical infrastructure industries included in that. I think that was a great step forward for us in prioritization of services.

Mr. KITTELL. I would say it is appropriate from our point of view from a legislative and a regulatory point of view to ask firms to address the risks that they identify, for example, in the outsourcing question earlier, that it is reasonable to take some sort of regulatory action vis-a-vis have you considered the complications of outsourcing and what have you done with it, as opposed to trying to write—which I think would be very difficult—write some sort of regulatory scheme around standards or principles or the way things need to be done, because each firm really has unique resources to play with, unique solutions to defend against these issues.

Chairwoman KELLY. My inclination is to agree with you. Before I came to Congress I noticed that every time Congress wrote a law it seemed to sort of foul things up a little bit. So maybe we can stay out of that and the industry can deal with it. Certainly it seems as though you have been dealing with it very well.

Mr. Schmidt, our final comment here.

Mr. SCHMIDT. Yes, thank you.

My recommendation would be for the committee to do as it has been doing, maintain the dialogue with those of us in the private sector that are the owners and operators of this, and I thank you for your leadership and the Congressman for his leadership in making sure that we, indeed, keep it to where the private sector can effect the changes without imposing regulations that probably do not work.

Chairwoman KELLY. Good, thank you.

This committee thanks all of you for staying here for such a long period of time. I appreciate it very much, and the Chair notes that some members may have additional questions for the panel. They may wish to submit them in writing. So without objection, the hearing record will remain open for 30 days for members to submit the written questions to these witnesses and place their responses in the record.

This second panel is excused, with our great thanks and appreciation for your time.

I want to briefly thank all the members and the staff for the assistance that they have given us in making this hearing possible.

This hearing is adjourned.

[Whereupon, at 3:52 p.m., the subcommittee was adjourned.]

A P P E N D I X

October 20, 2003

Statement of Chairwoman Sue Kelly
Subcommittee on Oversight and Investigations
“Government and Industry Efforts to Protect Our Money
During Blackouts, Hurricanes, and Other Disasters”
October 20, 2003

The recent blackout, which began on Thursday afternoon, August 14, left millions of Americans in the dark in many ways. Many were stranded at work, wondering how to get home. I know many of my constituents who work in the New York City did not make it home at all that night. Others were stranded at airports and transportation systems, wondering when to give up and find alternatives to waiting in dark corridors.

In the end, major cities from New City to Detroit were without centrally generated power; airports, water and sewage plants, and 911 emergency systems were shut down; and communications systems failed. It is now even clearer that the technology age we live in – which allows us to provide services and access information in a heartbeat – has increased our reliance on power. It is imperative that we review efforts to protect our systems and infrastructure that are evermore intertwined and dependent on one another.

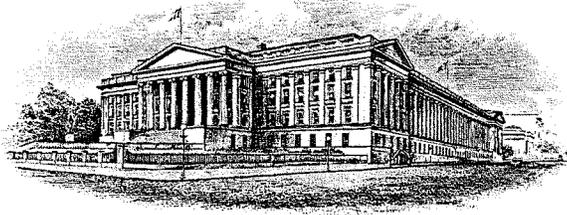
At the heart of critical infrastructure is the safety and soundness of the financial services sector. Fortunately, through all this, it appears that the financial services sector did not suffer any serious negative impacts. But we must use the recent blackout as a test to assess the security and dependability of our financial systems. Without doubt, there are lessons to be learned and improvements to be made.

Today, we welcome Wayne Abernathy, the Assistant Secretary for Financial Institutions at the Treasury Department, who will release a special report on the impacts of the blackout that will be crucial to how handle disasters in the future. Assistant Secretary Abernathy worked around the clock with many of our other witnesses here today to implement backup plans. Joining Assistant Secretary Abernathy on our first panel is Federal Reserve Board Governor Mark Olson who was also instrumental in these efforts.

Keeping our financial systems functioning and safe requires a high degree of coordination between many different and important parties – both public and private. The private sector witnesses on our second panel are leaders in protecting critical financial services assets from major disasters. These witnesses, along with others in the private sector and government who could not be represented here today, worked to ensure that our money supply and funds flow would not be jeopardized. The Depository Trust and Clearing Corporation, the New York Stock Exchange and NASDAQ, and associations, such as the Bond Market Association, played key roles to keep the markets working during the blackout. Many other agencies were also involved in addition to the Treasury Department and Federal Reserve System, including the Securities Exchange Commission. As the regulator of the nation’s largest financial institutions, the Supervisor of the New York State Banking Department, my good friend Diana Taylor, also played a key role. We thank the SEC and Ms. Taylor for their written statements submitted for the record.

We look forward to hearing the accounts of how our witness managed during the blackout, and how emergency plans for protecting critical infrastructure – which have been in place before September 11, 2001 – worked. There is no better indicator of the success of those plans than the fact that there was apparently no financial panic either during or after the blackout. We also want to hear how prepared the witnesses are for a major hurricane with these plans and whether Hurricane Isabel had any serious consequences.

I thank the witnesses for appearing here today and 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 confidence in the financial services sector.



**DEPARTMENT OF THE TREASURY
OFFICE OF PUBLIC AFFAIRS**

**Embargoed Until 2:00 pm EDT
October 20, 2003**

**Contact: Betsy Holahan
202-622-2960**

**Testimony of
Wayne A. Abernathy
Assistant Secretary for Financial Institutions
before the
Subcommittee on Oversight and Investigations
Committee on Financial Services
U.S. House of Representatives**

Good afternoon Chairwoman Kelly, Ranking Member Gutierrez, and members of the subcommittee. Thank you for this opportunity to testify today about the resiliency of the U.S. financial system. I am here today representing not only the Treasury Department, but also the Financial and Banking Information Infrastructure Committee (FBIIC), which is chartered under the President's Working Group on Financial Markets. The FBIIC is charged with improving coordination and communication among financial regulators, enhancing the resilience of the financial sector, and promoting communication and coordination with the private sector entities that make up and operate within our financial services sector. I represent the Department of the Treasury in chairing the committee. I want to thank all of the members of the FBIIC for their dedication and excellence in executing the mission set forth in our charter.

An old proverb suggests that experience is not always the kindest of teachers, but it surely is the best. Following significant threats to the financial infrastructure, the FBIIC makes it a practice to review what has happened, what went well, what did not, what can we learn, and what do we need to do. The FBIIC conducted such a review following recent events and compiled a written report, the "Impact of the Recent Power Blackout and Hurricane Isabel on the Financial Sector," which the FBIIC is releasing to the public today. I have submitted a copy of the report together with my remarks.

The U.S. financial system is remarkably resilient, as reaffirmed by such recent events as the Northeast power outage of August 14 and 15, Hurricane Isabel, and increasingly severe cyber-attacks. This resilience comes from many sources. One of them is vigilance. We have to continue to work to improve the resilience of the critical financial infrastructure of the United

States and the other critical infrastructures with which it is connected, such as the energy, telecommunications, and transportation infrastructures.

I would emphasize that our approach has been to begin and end by relying on the private sector. A central insight of the President's strategy to secure our critical infrastructure is that the infrastructure in this country is largely owned by private businesses. This is certainly true in the finance and banking sector. Accordingly, we pursue virtually all of our objectives in close collaboration with the private sector. I am especially pleased, therefore, that you have invited several important leaders of the private sector to this hearing to testify.

Both in preparation for potential disruptions to the financial infrastructure and in responding to actual threats, we are guided by four principles, in order of importance.

First, and most important, we must remember in all that we do to protect our financial infrastructure, that it is always about people. It is the people that make our financial institutions work, people that designed the systems, people that make them successful, people that innovate to keep them fresh and dynamic, and it is people whom they are designed to serve, people who rely upon financial services for so many aspects of their daily lives.

Second, because it is about people, it is about confidence. Our financial institutions operate on confidence, but they also promote confidence. In fact, confidence is what our financial institutions must provide, confidence that financial transactions will be carried out, that checks will clear, that bills will be paid, that investments will be made, that insurance promises will be kept. The confidence provided by financial institutions and their services play a big part in helping to cope with the trauma of disaster.

Third, essential to that confidence is open markets, financial institutions open for business, doing their business, allowing Americans everywhere to engage in their business, even during—especially during—times of stress. It is important for financial institutions and markets to continue to operate as close to business-as-usual as possible. During times of stress, investors need to price the effects of that stress on assets. The longer they are prevented from pricing the impact, the more anxiety builds and the worse the consequences will be when markets eventually re-open.

The fourth guiding principle is that we want to promote decentralized decision-making and problem-solving, both as we prepare for disruptions and as we weather them. In the event of a disruption to the payments system, for example, we want the payments systems experts to fix it. We do not want them to wait for guidance from Washington. Just fix it. The subject matter experts who are on the ground and in the field are in the best position to determine what steps should be taken to protect employees and customers. We will help where we can and where we need to, but we intend to leave the responsibility with the financial institutions and the regulators that are closest to the problems to find the solutions. Initiative and ingenuity are the most powerful tools to deal with any disruption, and we must give full room for their exercise.

Impact of the Power Outage of August 14-15, 2003

On Thursday, August 14, at approximately 4:11 pm, large areas of the Northeast lost power, including New York City, where a large amount of the U.S. financial infrastructure is concentrated.

The U.S. financial system handled the outage well.

The bond market and major equities and futures markets – with one exception – were able to open the next day for business at their usual trading hours.¹ The one exception, the American Stock Exchange, was able to open for a short, but important, trading session just prior to the normal market closing hour on Friday. Neither the Department of the Treasury nor any of our companion financial regulators received any reports of lost data, significant failed transactions, or other similar problems at individual institutions, exchanges, or the financial utilities that serve them.

Major market participants also performed well by keeping their systems up and running using power supplied by back up generators. The next day, major market participants traded in the currency, bond, equities, and futures markets. Although there were isolated reports of telecommunications difficulties between market participants and the markets or news services that supply real-time market data, the problems were minor and the participants and their telecommunications suppliers resolved these problems during the day.

Banks and credit unions also performed well. Although most branches and ATMs within the affected area were closed on Friday, there were no reports of lost or compromised data. In general, customers were able to briefly defer their banking transactions with little economic impact. The Federal Reserve System was fully prepared to make additional currency available to satisfy any increased demand for currency once power was restored. However, there was no significant increase in demand, and the Federal Reserve System did not need to implement fully its plan.

Impact of Hurricane Isabel, September 18-19, 2003

On September 18 and 19, some parts of the financial system were tested again, as Hurricane Isabel made landfall in North Carolina and moved across the Mid-Atlantic States. Isabel's impact on the financial system was significantly less than the impact of the power outage. For one thing, Isabel passed to the south and west of New York City and the surrounding metropolitan area, where much of the U.S. financial system is concentrated. For another, due to advanced weather reporting, the hurricane was not a surprise and the financial system had days to anticipate Isabel and prepare for its arrival.

¹ The bond market, through the Bond Market Association and with the support of the Department of the Treasury, closed at 2:00 pm on Friday to provide bond traders and the employees who support them additional time to get home. At the time, it was unclear when subway and train service would be restored, and most anticipated a difficult commute.

Although the impact of Isabel was less significant in degree, it was quite similar in kind to the impact of the power outage – both resulted in widespread disruptions of electric power and the businesses that depend on it. However, the storm neither adversely affected the financial markets nor the major participants in those markets. Similarly, although many bank and credit union branches and ATMs lost power, there was no significant economic impact from this: people did their business before the much-anticipated storm, postponed their business until power was restored, or drove to a nearby branch or ATM that had power – with no instances of lost or compromised customer data reported.

The Resilience of the U.S. Financial System

There are several reasons why the U.S. financial system fared so well in the face of the severe challenges posed by the power outage of August 14-15 and the somewhat less severe challenges posed by Isabel.

First and foremost, the men and women who work in the financial system did an extraordinary job. During the outage, many of these people stayed at their posts at financial institutions to ensure both that their systems preserved and processed data from trading on Thursday and that their systems would be prepared to resume trading the next day, on Friday.

Almost immediately after the power went out on Thursday, financial institutions began asking themselves not whether they would open for business the next day, but how they could best serve their customers' needs once open. By 6:00 pm on Thursday the major financial markets publicly stated that they would be open for trading during normal hours on Friday. This commitment to serve customers even in times of adversity is important. It gives customers confidence in using the U.S. financial system and, in turn, helps promote rational financial decisions by institutions and their customers.

I wish to note an important point in this regard. Financial institutions decided on their own that they would open for business the next day. They did not wait for guidance from Washington. They did not ask for permission to serve their customers. They decided for themselves. They knew how to serve the best interests of their institutions and their customers, and they acted accordingly. This is precisely the sort of private sector leadership and responsibility that we are promoting, and we were gratified to see it work so well during the power outage.

Third, financial institutions and their employees were well-equipped to continue their businesses in the face of challenges such as the outage. While no one foresaw the specific nature and dimensions of the power outage, careful planning and preparation helped financial institutions survive it. After the power went out, many institutions relied on these plans to switch to power supplied from back-up generators; and, in some cases, to switch to back-up data processing facilities located outside the impacted area. Although such planning and preparation has long been part of the best practices of running a safe and sound financial institution, it also reflects the benefits realized by the financial services sector as a result of increased investments in contingency plans, procedures, and equipment. Financial institutions have more alternative options available to them than they had in the past. During August 14-15, these investments paid off.

Fourth, good communications helped to remove uncertainty and maintain confidence. The President's early expression of confidence in the ability of officials, businesses, and citizens to weather the outage helped build resolve and maintain calm. Mayor Bloomberg and his team also did a superb job of providing a range of emergency services and communicating the impact of the outage and their response clearly and confidently not just to the citizens of New York, but to the world. Financial institutions communicated well among themselves and with their regulators.

Finally, the regulators communicated efficiently and effectively among themselves and with the private sector. For example, shortly after the power went out, Treasury convened a conference call of the FBIIC, waiting just long enough for regulators to gather detailed information about the impact of the outage on Thursday's activity and the likely impact on Friday's activity. This conference call provided an early opportunity for the regulators to share information about the impact of the outage on each of their regulated sectors. As that information was, in turn, passed to major participants in the sectors it further helped the industry manage the impact of the outage. As another example, the private sector counterpart to the FBIIC, the Financial Services Sector Coordinating Council (FSSCC), convened a series of conference calls that enabled the financial sector to gain valuable, up to the minute information about power restoration which helped them prepare for the next day's activities.

Lessons Learned and Next Steps

Although the U.S. financial system weathered the power outage of August 14-15 and Isabel well, the Department of the Treasury and our companion financial regulators in the FBIIC have extracted some lessons learned and identified steps to take next as we work with our partners in the financial industry to further improve the resilience of the U.S. financial system.

Need for Additional Work on Inter-Dependencies

The power outage highlighted some of the inter-dependencies of our critical infrastructure. The critical financial infrastructure, while extremely resilient, is also dependent on other infrastructures including energy, telecommunications, information technology, transportation, and others. These interdependencies were made all too clear by the attacks of September 11, 2001 when a vault containing a large number of telecommunications lines was destroyed. Financial institutions that purchased redundant lines from multiple carriers were surprised to learn that because many of the lines were routed through that same vault, they had much less telecommunications redundancy than they thought.

Since September 11, the financial industry and the telecommunications industry have made important strides toward improving the resilience of the telecomm infrastructure on which the financial services industry depends. For example, some exchanges, the key financial clearing and settlement facilities, major market participants, and telecommunications companies have created a dedicated, self-healing telecommunications network. More work is underway in this area

Another important interdependency exists between the financial services sector and the information technology sector. By many accounts, the financial services sector is one of the largest consumers of information technology products and services. The financial services industry uses information technology not only to operate critical business processes, but also to communicate with its customers and, in many cases, to distribute products. This use of information technology contributes, of course, to the remarkable productivity, ingenuity, and resilience of the U.S. financial system. At the same time, the heavy reliance upon information technology renders the U.S. financial system – like the financial system of many other nations – potentially vulnerable to cyber attacks. Over the past nine months, worms and viruses like Slammer, Bugbear, and Sobig.F, have challenged administrators of financial institutions' computer networks. Moreover, these attacks are not only becoming more sophisticated, they tend to spread more quickly and are occurring with greater frequency. It is clear that the financial services sector is an attractive target. For example, the Bugbear worm specifically targeted over 1600 financial institutions around the globe, with the apparent intent not just to disrupt transactions, but to steal funds.

Much work is underway to protect our critical financial infrastructure from cyber attack, and I would like to share some of these efforts with you.

As the first line of defense and responsibility, financial institutions shoulder the job of minimizing the vulnerabilities within their own systems. This responsibility is reinforced by the financial regulators, whose examiners inspect banks and other institutions for safe and sound practices, including “technological safeguards” required under Section 501(b) of the Gramm-Leach-Bliley Act.

To assist in the promotion and communication of best practices, as well as to assist in the dissemination of advisories, the Financial Services Information Sharing and Analysis Center (FS-ISAC) is expanding the reach of its communications network to nearly every financial institution. The Department of the Treasury was pleased to support the FS-ISAC in the development of this next-generation plan, and we look forward to supporting the FS-ISAC as it implements the plan.

Moreover, to assist in crime deterrence and apprehension of cyber crooks, the Treasury has been pleased to support and work with the United States Secret Service as it creates electronic crimes task forces across the nation. Just last week, my Deputy Assistant Secretary for these issues participated in the official roll-out of such a task force in Cleveland. We look forward to continuing efforts with Director Basham and others in the United States Secret Service in this important area.

Still more needs to be done to protect the financial sector from cyber attack. Two immediate priorities include reducing the number of vulnerabilities introduced into software products and addressing potential vulnerabilities introduced by the business practice of domestic and international outsourcing of customer service, data management, and software development.

Conclusion

The U.S. financial system is more resilient today than it was a year ago. The men and women who work in the system help make it so. Our job is not finished. It is a big job. To paraphrase Winston Churchill, we are not at the end, or even the beginning of the end. But we might be nearing the end of the beginning. Americans and the world can rely with increasing confidence on the U.S. financial system.

42

STATEMENT

OF

CATHERINE A. ALLEN

CEO

BITS

BEFORE THE

HOUSE COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

UNITED STATES CONGRESS

HEARING ON
GOVERNMENT AND INDUSTRY EFFORTS TO PROTECT OUR MONEY DURING
BLACKOUTS, HURRICANES AND OTHER DISASTERS

OCTOBER 20, 2003

TESTIMONY OF CATHERINE A. ALLEN, CEO, BITS

Introduction

Thank you, Chairwoman Kelly and Ranking Member Gutierrez, for the opportunity to testify before the House Committee on Financial Services Subcommittee on Oversight and Investigations about the ways the financial services sector is addressing customer and industry needs during disasters such as the recent power outage in the Northeast.

I am Catherine Allen, CEO of BITS, a nonprofit industry consortium of the 100 largest financial institutions in the US. BITS is the sister organization to The Financial Services Roundtable. BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS is not a lobbying organization. Our work in crisis management coordination, cyber security, critical infrastructure protection and fraud is shared not only among our member companies but throughout the financial services sector. BITS works with other critical infrastructure sectors, government organizations, technology providers and third-party service providers to accomplish its goals.

BITS was holding its Advisory Group and Council meetings in Detroit at the time of the August power outage. I was there along with the Chief Technology Officers and other senior executives of many of the nation's largest financial services firms. My direct involvement in our industry's efforts is the basis for my belief that our financial system and communications worked well despite the challenges of being without power, landline telephones and water.

Power Outage Impact

BITS member companies and customers experienced the outage in Detroit, as well as in New York and other Northeastern states with a high concentration of financial institutions. **Bottom line, the financial services industry and our customers fared well. Backup systems worked, 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. However, there were “lessons learned” that require follow-up.

Let me outline **three major reasons why I think the nation’s financial system fared so well:**

- **Preparation** – The events of 9/11 and subsequent preparations by the private sector and government enhanced our trust in each other and our ability to communicate, shift to backup systems, and continue operations. BITS, in fact, 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 helped us think through things like communications, water shortages, backup for ATM operations, and fuel for generators.
- **Early announcements that this was not a terrorist event** – This helped to alleviate 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”—where external communications to institutions are blocked—might have occurred. Early understanding of the scope of the blackout and confirmation that it was not terrorist related were critical.
- **Diversity of communications** – Although landlines and some cell phones were knocked out of use or could not be recharged, we did communicate through diverse channels such as Blackberries, which have long charge lives and generally work well in urban areas. In fact, Assistant Treasury Secretary Wayne Abernathy and I communicated through the evening of August 14 by Blackberry. Mr. Abernathy helped get important government players on the telephone for a BITS and Financial Services Roundtable hosted call that night at 10pm during which industry and government representatives were able to discuss the events of the day and assess the potential impacts, such as whether markets would open on that Friday.

There were several **critical lessons learned from the event:**

- **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 can not be overstated.

- **Water for cooling systems and personal hygiene often is powered by electricity.** Many companies, for example, did not have backup generators for water supplies. This caused several organizations to close their offices or delay opening.
- **Communications must be viewed as an integrated system.** Diverse elements—cell phones, Blackberries, landline phones, and the Internet—are required. We must understand the vulnerabilities and mitigate them. Both diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services will be maintained.

Attached to this testimony are a wide variety of lessons learned and our resulting specific recommendations gathered from our members' experiences during the outage. These were compiled after several conference calls of the BITS Crisis Management Coordination and Information Technology (IT) Service Providers Working Groups. The highlights and recommendations revolve around:

- Contingency Planning and Third-Party Service Providers
- Communications
- Coordination with Federal, State and Local Governments
- Access to Transportation, Water and Fuel

The Interdependency Issue

The most important lessons learned from the outage are how interdependent the critical infrastructures are and how fortunate it is that we did not have an event that was terrorist-driven or involved a simultaneous cyber security attack. We need to look strategically and holistically at the nation's critical infrastructures and what can be done to enhance resiliency and reliability.

Since 9/11, BITS has intensified its focus on this issue of interdependency and cascading events, especially where potential terrorist events may occur on multiple fronts. Our focus is in four areas:

1. Telecommunications vulnerabilities and recovery capabilities
2. Business continuity, crisis management best practices, and cross-industry coordination.

3. Security practices of outsourcers.
4. Security criteria for software in the development phase, as well as less frequent and more effective patch-management processes.

BITS is addressing **interdependency issues with the telecommunications industry**. BITS has led an effort on behalf of the financial services industry focused on assessing telecommunication vulnerabilities and enhancing recovery. The telecommunications and financial sectors are demonstrating unprecedented cooperation, supported by the National Communications System (NCS) of the Department of Homeland Security (DHS). The NCS and the DHS have been exceptionally helpful in bringing our two industries together to address diversity, redundancy, and recovery. Results of our 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 policies
- Pilots to model the costs of attaining greater diversity and redundancy in telecommunications services to the financial services industry
- Adoption by BITS and Financial Services Roundtable CEOs of the Network Reliability and Interoperability Council (NRIC) best practices in physical and cyber security
- Education of both sectors on the importance of working closely together to identify and address issues

In the **crisis management coordination** area, BITS utilizes the Crisis Communicator, a high-speed, automated alert system that allows BITS and The Financial Services Roundtable to bring together CEOs, CIOs, crisis management executives and government officials in a matter of minutes. We developed potential scenarios and manuals for cross-industry coordination. We participate in the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). We created, on behalf of the FSSCC, and jointly with the Securities Industry Association (SIA), best practices for responding to the DHS Alert Levels Yellow through Red. Through the FSSCC, these efforts have been shared throughout the financial services industry as well as with other critical infrastructure industries.

BITS' **IT Service Providers Working Group** created the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships*. This document provides the financial services industry and service providers with risk-management strategies for evaluating outsourcing opportunities and helps them to meet regulatory requirements. We will be releasing a Security Assessment Matrix through which companies can standardize to make more rigorous their requirements for security and protection of data from vendors and service providers. This, too, is available to others in our industry, as well as to the audit and assessment and vendor communities.

In the area of **software security**, BITS has created the BITS Product Certification Program (BPCP), a testing capability that provides security criteria against which software can be tested. BITS has also launched a best practices effort for patch management and is launching a “user-driven” coalition effort to address software-development processes and patch-management procedures at a CEO-to-CEO level. We will get back to you with recommendations in this area by early next year.

We urge the Committee to consider all aspects of critical infrastructure—the software and operating systems, the service providers, the critical infrastructure industries, and the practices of firms, industries and the government—in addressing not only power outages but future disaster-related events.

Recommendations

We have developed five key recommendations for the Committee to consider:

1. **Invest in the power grid** because of its critical and cascading impact on other industries and other critical infrastructures. In fact, there needs to be investment in all base critical infrastructures—power, telecommunications, transportation—to provide business continuity and critical economic recovery in the event of a crisis. Incentives such as credits for investments, research and development subsidies, tax reductions and direct government investment should be explored.

2. **Announce early whether an event is terrorist-related or not.** This information is critical to the execution of crisis management procedures and communications to maintain public confidence.
3. **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.
4. **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.
5. **Recognize and review the dependence of all critical infrastructures on software operating systems and the Internet.** A cyber attack of some kind which impacts communications, SCADA systems or first responder systems would put all of us at terrible risk. Compounding the problem is the lack of security in software development and the current inefficient software patch processes that cause our industry to spend millions of dollars that could be better used for enhancing security and business-continuity practices. This is an alarming issue and critical to protecting the nation’s infrastructure. 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.

On behalf of both BITS and The Financial Services Roundtable, thank you for the opportunity to testify before you today. I will now answer any questions.



LESSONS LEARNED: NORTHEAST BLACKOUT OF 2003

Compiled by the
**BITS Crisis Management Coordination and
 IT Service Provider Working Groups**

This document highlights key lessons learned from the power outage that affected the Northeast from August 14 through 16, 2003. It was compiled based on a series of conference calls with members of the BITS Crisis Management Coordination and IT Service Provider Working Groups as well as published articles about the event and its implications. This document does not represent the efforts of the other financial services industry associations and/or coordinating bodies. This only reflects the BITS perspective and lessons learned relevant to our crisis management coordination process and our members' experiences. BITS is a nonprofit industry consortium that shares its membership with The Financial Services Roundtable. BITS serves as the strategic "brain trust" for the financial services industry in the e-commerce, payments and emerging technologies arenas, and also facilitates cooperation between the financial services industry and other sectors of the nation's critical infrastructure, government organizations, technology providers and third-party service providers.

In general, the nation's financial services sector withstood the massive power outage with little or no disruption. Verification and notification by Department of Homeland Security (DHS) officials that the power outage was not terrorism-related provided the public with important assurance. Clearly, the nation's power grid and transmission network should be strengthened to prevent power outages of this magnitude. Further research is needed to understand whether software security weaknesses contributed to the outage.

Contingency Planning and Third Party Providers

- Financial institutions relied on business continuity plans to respond to the power outage and related consequences.
- Data-protection schemes worked almost flawlessly for most large companies affected by the power outage. Recovery planning efforts made by financial institutions since 9/11 enabled them to respond to the crisis effectively.

Recommendations

- Ensure all critical systems are located in facilities with adequate backup power capacity.
- Evaluate single points of failure, redundancy, and single-provider implications.
- Evaluate, define and test procedures for operating and restarting equipment during power failures.

- Ensure financial institution patch-management programs include software at contingency sites or vendor-controlled sites.
- Validate emergency building access policy/procedures with third-party building management services.
- Establish and maintain strong relationships with critical partners and suppliers such as power, water, and telecommunications providers.
- Maintain quick-ship/contingency agreements with suppliers.

Communication

- Overall, the BITS/FSR crisis notification process worked well.
- Due to the large number of conference calls at certain times, some key individuals could not participate in conference calls.
- Individuals with strong facilitation skills should lead calls in a quiet location.
- Many member organizations have automated notification systems that provided paging services and 800 numbers for associates to use to receive information.
- Alternate communication devices allowed financial institutions to communicate with employees, third parties, customers and regulators. With limited cell phone service, Blackberries became a primary and important means of communication for many members whose internal communications servers were not disabled.
- Most Government Emergency Telecommunications Services (GETS) Cards worked.
- Some satellite phones did not work in the New York City area because tall buildings and other environmental factors can affect the phones' ability to receive a signal.
- Reported telecommunications problems included inadequate backup power at telecommunications companies and a spike in the volume of calls. (In the hours after the blackout hit, leading wireless carriers reported three to four times the normal volume of calls, a load that virtually guaranteed that many people would hear busy signals and not be able to get through.)
- Many cell tower generators failed due to insufficient fuel to operate and support the increase of wireless communications. Many of the trucks that service these towers depend on commercial power to refuel and encountered roadblocks in their attempts to reach the towers. The National Coordinating Center of the National Communications System coordinated efforts to get the trucks through the roadblocks and helped secure generators for those carriers in need.
- Because so many thousands of servers were effectively "removed" from the Internet so quickly, it caused a sustained surge in BGP (Border Gateway Protocol) traffic to update router tables, effectively blocking other traffic temporarily and slowing the Internet.

Recommendations

- Obtain as many means of communication with key individuals at third-party service providers as possible (including home phones, cell phones, and email addresses).
- Ensure alternative communication channels to communicate with the media, third party providers, customers, and government agencies.
- Develop an improved system for communicating emergency and building evacuation instructions and employee protocols.

Coordination with Federal, State and Local Government

- Government officials provided accurate and timely information, which helped to maintain order. Increased presence by public safety officials helped to alleviate fears and minimize looting and civil unrest.

- Overall communication between government officials and the private sector was successful. Officials from the Federal Reserve, DHS, and Treasury were very responsive to BITS' requests for information and coordinated effectively with the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC).
- All of the major cities affected by the blackout had post-9/11 emergency procedures in place. When electric water pumps shut down in Cleveland, authorities tapped private water trucks the city had arranged to be available in emergencies. Communities in suburban Detroit collaborated to evacuate residents living near a potentially dangerous gasoline plant.

Recommendations

- Establish and maintain strong relationships between the industry and federal, state and local governments.

Transportation, Water and Fuel

- There was widespread disruption to transportation systems, including trains, subways and air travel. Limited and often conflicting or inaccurate information was provided to air travel customers.
- Some companies encountered problems with armored car companies or courier services that would not deliver to locations where power had not been restored. Additionally, some couriers could not gain access to areas due to curfews – or were not able to obtain fuel to complete deliveries.
- Some companies reported a shortage of fuel for generators and difficulty in obtaining additional fuel for their generators.
- In some states, water supplies were affected because water is distributed through electric pumps.
- The inability to pump water and use electronic flushing devices rendered many buildings uninhabitable. High-rise buildings were evacuated due to their inability to run fire pumps.

Recommendations

- Ensure there is adequate food and water at key locations.
- Ensure ATMs in key locations have an alternative power source in the event of a power failure.
- Ensure that critical business units/facilities functions are adequately supported by generators.
- Test generators regularly at full capacity for extended periods of time.

**Testimony of
Donald D. Kittell
Executive Vice President
Securities Industry Association**

**"Government and Industry Efforts to Protect Our Money During
Blackouts, Hurricanes and Other Disasters"**

**Before the
U. S. House of Representatives Committee on Financial Services
Subcommittee on Oversight and Investigations**

October 20, 2003

Opening Remarks

Chairwoman Kelly and Ranking Member Gutierrez, I am Donald Kittell, Executive Vice President of the Securities Industry Association, thank you and I appreciate the opportunity to discuss the impact on the securities industry of the August blackout and Hurricane Isabel.

Since the 9/11 terrorist attacks, the securities industry has invested significant time and resources in its business continuity plans. The opening of the financial markets on Friday, August 15, the day after the blackout, clearly demonstrated the viability of these plans. A month later, the threat from Hurricane Isabel further tested the effectiveness of our pre-event preparation strategy. There were specific lessons for us in each case.

I will address most of my comments to the blackout situation because it had a significant impact on the securities industry. Hurricane Isabel had nowhere near the impact on New York as it did in Virginia, North Carolina and here in Washington, but there were implications for us here as well.

Industry Response

Overall, the securities industry's response to the blackout was successful. The support we received from city, state, Federal and regulatory bodies was exemplary.

When street power was lost, there was a seamless transition to backup power sources by firms and exchanges.

SIAC processing for the New York Stock Exchange, the American Stock Exchange, the National Market Systems, Depository Trust Clearing

Corporation and Fixed Income Clearing Corporation was uninterrupted and completed within normal time frames. When the blackout occurred, SIAC's sites were protected by UPS (battery) power combined with backup generators. There were no interruptions in processing, and no loss of data.

The Depository Trust & Clearing Corporation activated both its remote data center and its remote operating location. On Friday, all IT production took place at the NYC data center, but was controlled completely by the remote data center. Similarly, business operations were managed by the staff at the remote operating location although a large portion of the staff worked at the NY offices. This proved to be an important and successful test of DTCC's remote operating capability, which was developed after 9/11.

When the blackout occurred on August 14, the American Stock Exchange immediately implemented emergency procedures and activated back-up generators. By 1:00 a.m. the following morning, the Amex building and trading systems were fully powered and operational. The trading floor cooling system and its support technology, however, rely on steam from the Con Edison New York City steam grid, which was completely shutdown by the power outage. With help from the City of New York Office of Emergency Management, the Amex obtained emergency steam-generation boilers and conducted a delayed opening on August 15. Amex was able to establish firm closing prices for its products on August 15.

Some securities firms reported that they elected to relocate some personnel to contingency sites for business the next day. Many firms functioned under split operations plans, where the primary sites remained operational. All firms and exchanges opened on the day following the blackout.

SIA activated its command center within minutes of the blackout. The command center uses pre-determined contact numbers to assemble more than 80 BCP professionals from critical industry organizations. Once connected, these professionals share information about causes and back-up steps taken by each. The command center conducted conference calls throughout Thursday night, the following Friday and into the weekend.

SIA has maintained a seat at the New York City Office of Emergency Management since the Y2K conversion. Our seat is staffed throughout every major emergency and was activated for both the blackout and the hurricane. This arrangement facilitates a timely, effective flow of information and provides for communications among city and state government organizations, utility service providers and industry. It provides a mechanism to resolve unforeseen issues that may affect our recovery process. The OEM's ongoing relationship with SIA and representatives of other NYC industries is invaluable.

Recovery Coordination Issues

In the event of an emergency, SIA coordinates among financial services firms, exchanges, regulators, industry utilities and other industry organizations to facilitate the prompt restart of the trading process. Over the past few years, the number of conference calls necessary to accomplish this has grown. During the blackout, we experienced situations where multiple calls were set at the same time or calls intended to gather information were scheduled after the calls that were to disseminate that information. The industry and regulatory agencies are working to further coordinate these calls.

Despite the large number of organizations currently involved in this process, we believe there is value to adding others including telecom carriers, power companies, service bureaus and market data vendors.

Infrastructure Issues

Through its contingency planning process, the industry fully anticipated an event that included loss of power. The widespread, simultaneous loss of communications and transportation presented the most difficult challenges.

Cell phone service was found to degrade after several hours. This has been attributed to increased call volume compounded by the fact that many cell nodes currently have only battery backup power for a few hours, but not longer-duration generator power. In addition to cell phone service issues, telephone landline communications were lost when switching stations in Brooklyn and lower Manhattan became disabled. The securities industry relied on other communications resources including Blackberrys and two-way radios.

The communications and electric power utilities responded quickly to invoke their emergency plans. It is worth noting, though, that utility providers operate under somewhat less stringent recovery time objectives than those required of the financial services industry. Had the event occurred during trading hours, achieving full recovery of the securities markets, especially without communications services, would have been challenging.

The shutdown of Con Ed steam generation facilities for the first time in 123 years and the length of time required to restore service, highlighted the importance of this resource in New York City. Steam is generally thought of as a source of heat, but it is also used to drive the air conditioning systems in some buildings. During the blackout, all six Con Ed steam plants were disabled and service could not be fully restored until the entire transmission pipe system was purged. The securities industry, New York City and Con Edison are addressing steam reliability as a priority issue.

Although financial services firms did not experience problems refueling their generators, instances were identified in the New York area where delivery trucks could not be reloaded because pumps at the depots had no backup power. This would certainly pose a problem during a longer-term outage and is being studied further.

In NYC, most transportation systems were immobilized and many employees were stranded in the city overnight on streets and in public places. Although ferries continued to operate, they were overwhelmed by the number of riders and were not able to transport all passengers off Manhattan until the following morning. As a result, many firms are considering a "Stay in Building" policy to allow and encourage at least critical employees to remain on-site. SIA reported to the OEM on the need for a stronger police presence at ferry terminals during emergencies to control overcrowding situations.

Government Liaison Issues

The event did emphasize the value of a system that would allow critical personnel to have limited access to restricted emergency zones after a disaster. Being able to retrieve critical records and equipment is often essential to the recovery process.

New York City and New Jersey have been considering the use of pre-authorized emergency access credentials for limited numbers of employees of critical firms. After the blackout, SIA encouraged the NYC Corporate Emergency Access System (CEAS) to be fully approved and implemented. Since then, NYC approved the CEAS plan and is moving to implement it.

Hurricane Isabel

In September, the financial services industry in New York faced the threat of Hurricane Isabel tracking near or through the area. Because a large portion of the Wall Street financial district is situated in "Evacuation Zone A", the lowest-lying areas of the City that are the first to be evacuated, our business continuity plans are particularly attuned to potential high water situations.

The New York City OEM monitored this storm for more than a week prior to landfall and provided ongoing reports to private industry about its potential effect and the City's emergency plans. Several days before its expected arrival, OEM activated the City's Emergency Operations Center. SIA staffed its seat throughout the emergency.

Although the storm did not impact New York, the event allowed us to test and validate the emergency preparation component of our plans. The activation and the operation of the EOC was a good example of how to deal with an event of this kind.

Conclusion

In some ways we were lucky that both the blackout and Hurricane Isabel transpired as they did.

The blackout occurred after trading hours. Had it happened earlier in the trading day or prior to the opening, we would have faced different challenges - challenges of operating the markets with limited voice communications support and the challenge of getting employees to work with limited transportation.

Hurricane Isabel tracked farther to the west than originally projected and had no significant effect on New York. We are well aware, though, that a direct hit could have resulted in not only a blackout situation, but wind and flood conditions as well.

Our post event reviews highlighted potential improvements to our recovery strategies along with some limitations of the support infrastructure in New York. But, they also tell us that we can recover effectively from events far more significant than those we faced over the past two months.

Since 9/11 the financial services industry, in partnership with federal, state and city emergency management organizations, regulatory agencies and service providers, has vastly improved its resiliency. We are proud of progress to date and we continue to seek out and address potential vulnerabilities as an integral part of our overall business continuity plans.

Thank you.

STATEMENT OF RHONDA MACLEAN

Chairwoman Kelly, Ranking Member Gutierrez and members of the Subcommittee, thank you for inviting me here today to testify at this hearing on "Government and Industry Efforts to Protect Our Money During Blackouts, Hurricanes, and Other Disasters." I am honored to appear today to speak on behalf of the financial services sector in my role as the Department of Treasury-appointed private-sector coordinator for critical infrastructure protection.

My name is Rhonda MacLean. I am a Senior Vice President at Bank of America Corporation responsible for Corporate Information Security. My responsibilities also include serving as a member of the Bank of America Business Continuity Executive Team. This executive team oversees business continuity at Bank of America and acts as the senior management team when a major disaster recovery response has been activated.

Before joining Bank of America in 1996, I worked for The Boeing Company for 14 years, and as the senior manager for computer and communications security, I was responsible for all commercial airplane and government information security initiatives. I have served in a number of external advisory roles and in professional activities related to information security; I currently serve on the University of North Carolina – Charlotte, Board of Advisors for the College of Information Technology. My sector coordinator appointment does not involve receiving any federal funds.

Today, I plan to provide you with brief background on the financial services industry's involvement in critical infrastructure protection and the current work of our Financial Services Sector Coordinating Council. Also, I will describe, at the sector level, how the federal government and industry are working together to protect and respond in a coordinated manner to events that could affect operations of critical financial services provided by our sector. At all levels across our sector, including executive leadership, operations personnel, our trade associations, and professional institutes, and our customers, we are acutely aware of the new global realities and the importance of the vital financial services we provide globally to the nation and our customers.

Historical Perspective

During the past six years, elements of U.S. government policy and initiatives have increasingly focused on infrastructure protection. Encouraging an active public-private partnership has been a hallmark of their strategy.

Historically, the financial services sector has been a leader in addressing the challenges associated with operating the vast array of information technology and processing inherent throughout the financial services industry and infrastructure. Vigilance and the dedication of significant resources, over time, have allowed us to develop a wealth of expertise, experience and talent to address issues of security, risk management, disaster preparedness and business continuity.

To address the many recommendations proposed in the President's Commission on Critical Infrastructure Protection report, an action plan was developed in May 1998: the Presidential Decision Directive (PDD) 63. The primary banking and finance sector goal established in PDD-63 was to ensure the orderly functioning of the economy and the delivery of essential services.

The events of September 11, 2001, and the creation of the Department of Homeland Security in 2002 further increased focused efforts toward preparing for events that could impede orderly operations of the nation's financial systems.

In April 2003, the Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and the Securities and Exchange Commission issued the "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System." This paper identified sound practices focused on minimizing the immediate systemic effects of a wide-scale disruption on critical financial markets.

Let me discuss how our sector-level critical infrastructure protection efforts have evolved over the last year.

Financial Services Sector Coordinating Council

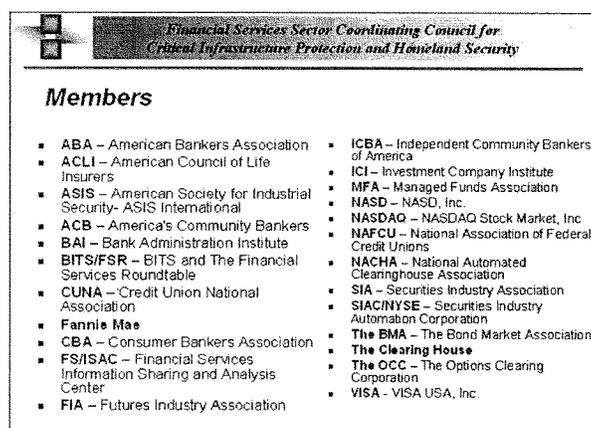
At the time of my appointment, no single entity represented the financial services sector. Individual associations were effectively working on their members' behalf to provide tools and resources necessary to enhance infrastructure protection. The associations and their members have provided much leadership for our sector and have done outstanding work in various areas, including crisis management efforts, "good practices" knowledge sharing, business continuity practices, and education and awareness initiatives.

Immediately after my appointment as sector coordinator by the Treasury in May 2002, we began forming the Financial Services Sector Coordinating Council, with the public sector's support and encouragement, and with the Treasury's leadership. I want to recognize Treasury Assistant Secretary Wayne Abernathy and Deputy Assistant Secretary Michael Dawson for their instrumental leadership in promoting and supporting an effective public-private sector partnership that is serving as a model for other sectors. Our Council members and their organizations, highly value the contributions they are making.

The council consists of the primary organizations that, through their constituencies, represent the majority of the financial services sector. These include key national

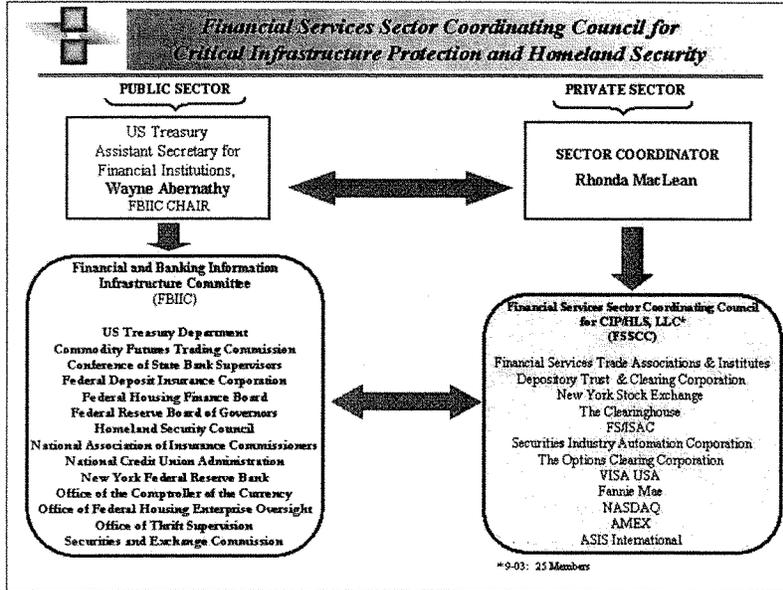
exchanges; clearing organizations; trade associations in the banking, securities, bond, and insurance segments of our industry; and key professional institutes.

Today, 25 organizations, listed below, are working together on behalf of their constituencies to identify and coordinate strategic initiatives for improving critical infrastructure protection for our sector and with the other sectors upon which we depend. The council is a limited liability corporation that has been institutionalized to carry on the sector's work long after my tenure as sector coordinator is completed. Through our council members, we engage nearly all financial services sector institutions, exchanges and utilities.



At the sector level, this is an example of 'macro' collective leadership being taken to address the new realities. Through this collective leadership and collaboration, we are leveraging the work being performed across the sector for the benefit of the "common good" of our industry. Other national critical infrastructure sectors are examining the council model and approach being taken by our sector.

This council provides an efficient approach for coordinating the efforts of the many, diverse participants that comprise our industry sector. Additionally, we have an opportunity for direct dialogue on common issues and challenges with a corresponding group within the public sector, the Financial and Banking Information Infrastructure Committee (FBIIIC), chaired by the Treasury Department. The result is an emerging agreement on strategic initiatives we believe will improve infrastructure protection and homeland security.



The council's work currently focuses on five strategic areas. Our approach is to leverage the work our member organizations have already accomplished to achieve our objectives. Council members are taking primary leadership roles in these areas based on their natural areas of expertise.

Information Dissemination and Information Sharing – The goals are to both ensure a universal service to disseminate trusted and timely information will be available to all sector participants; and to increase knowledge about physical and cyber security operational risks faced by the financial services sector. A major focus of our current sector efforts is toward enhancing the needed services provided by our sector's ISAC. Under the Department of Treasury's leadership additional funding is being obtained to assist in the enhancements of the next generation ISAC, bringing increased service and functionality that will meet the diverse needs of the sector. This partnership has been instrumental in helping the sector reach our goals.

As an interim step in ensuring we are able to reach the breadth of the sector with urgent alerts and warnings, the Financial Services Sector Coordinating Council, has implemented through the Council member associations the distribution of the important

alerts. In the last two quarters we have gone from approximately 70 financial institutions receiving this important information to over 8,000 today. This is a significant step forward in our goal to ensure trusted timely information dissemination.

In addition, comprehensive marketing strategy to promote awareness and active participation by all members of the Financial Sector is in process with a major campaign scheduled to begin the 1st quarter of 2004.

Crisis and Response Management – When events occur with broad sector or national impact, a planned and adopted approach for sector-wide crisis management coordination must exist, including coordination with government entities. Our efforts focus on improving the ability to communicate and respond as a sector when such events occur.

The Council uses a “Crisis Communicator” capability that allows Council members to convene in times of emergency. You will hear more about how this process combined with other communication processes that support sector and cross-sector communications.

Sector and Cross Sector Outreach – It is important for each organization to determine how to optimally support and commit efforts for achieving the goals of the executive orders and national strategies. We are developing a strategy for sector-wide outreach on homeland security and critical infrastructure protection initiatives that includes regional forums we are conducting jointly with the FBIIC. This effort, coordinated by the Federal Deposit Insurance Corporation (FDIC), has already occurred in four cities this year; Chicago, Dallas, San Francisco, and Los Angeles, and twenty more similar events are being planned for completion by the end of next year. The Council members also provide leadership and support to various regional business continuity initiatives such as the Chicago First group and the New York Office of Emergency Management.

Knowledge Sharing - Best Practices – There are numerous “lessons learned” activities and knowledge sharing of “good practices” within various trade associations and among institutions and government entities. We are developing an organized repository to provide this information to authorized institutions and individuals.

National Strategy – We are also leading the sector’s effort to revise our sector’s “national strategy” document in response to the two national strategies President Bush released in February. Our strategies are focused on “The Physical Protection of Critical Infrastructures and Key Assets” and “Securing Cyberspace.” This is our opportunity to define strategic as well as tactical, actionable and measurable programming, to direct and advance our sector-wide critical infrastructure and homeland security efforts and to address recommendations outlined in the national documents’ strategies referenced above.

In my role as Chairperson for the Sector Council, I work closely with our lead agency, the Department of Treasury, and the Financial and Banking Information Infrastructure Committee (FBIIC).

Through council members' cooperative efforts, their member institutions, and the strong leadership provided by the Treasury and through FBIIIC, we are able to maximize our resources and achieve our objectives to ensure our critical infrastructures are protected, for the benefit of the economy and for all financial services customers.

Increased Cross-sector Coordination

The sector coordinators appointed for the various infrastructures meet together regularly. In addition, the Sector Coordinators work in partnership with Department of Homeland Security (DHS) through the leadership of Undersecretary Frank Libutti. The purpose of these meetings is to focus on cross sector issues, best practices and opportunities to improve overall resiliency for our nation's critical infrastructures. The personal relationships developed among sector coordinators and with DHS had a material benefit during the August Blackout. Additionally, the various sector-level Information Sharing and Analysis Centers (ISACs) are examining ways to better share information among their activities.

Financial Sector Leadership and Preparedness

Following the September 11 tragedy, many financial sector institutions and organizations have reexamined their business continuity preparedness and improved their crisis management coordination and communications. As a practice, each event has offered opportunity to seek continuous improvement in our preparedness.

We have continued a strong partnership with our government partners and continue to get incredible support from the Treasury and other FBIIIC members, which enable us to accomplish our strategic objectives. We have had numerous opportunities to share with other sectors and with DHS, the benefits of our model of partnership between the FBIIIC and the FSSCC that enables our success.

We have also had numerous opportunities to test our crisis management procedures at a sector level and at the association level. If we examine the August Blackout, which had a larger geographic impact than hurricane Isabel from a power outage perspective, we came through these events beautifully but also with lessons learned. These lessons learned provide opportunity to focus on improving our sector-wide coordination to ensure the ongoing protection of our infrastructure. The Department of Homeland Security, Department of the Treasury, Financial Services Roundtable/BITS, Securities Industry Association, Financial Services Information Sharing and Analysis Center, The Depository Trust & Clearing Corporation, The Bond Market Association, as well as others, were most noteworthy in assessing the situation during this event and coordinating decisions among leaders within our industry.

As sector coordinator, I was able to participate or receive information from each of these activities during conference calls with the groups' leaders. Additionally, because of the close working relationships developed while working together on critical infrastructure protection initiatives, our sector received regular status updates on restoration activities

and timelines from Mr. Michehl Gent, Sector Coordinator for the Electric Power sector and President of the North America Electric Reliability Council (NERC), and his staff. This level of direct communication is invaluable, as efforts occurred to evaluate the situation and plan next steps.

Assistant Secretary of the Treasury Wayne Abernathy and FBIIC members performed a post-blackout review in which a number of private sector organizations participated. Overall, the financial sector business continuity preparedness and wide application of backup generators and systems were able to operate without any significant disruption until power was restored. Many of the details are being covered in my sector colleague's testimony.

Many non-essential personnel were evacuated from affected areas without incident. Most data centers switched over to emergency power, resulting in no disruption to clearing and settlement system activities. Some fuel deliveries occurred during the night to ensure adequate long-term emergency power in the event of a prolonged outage.

With power restored to critical locations before start of business the next day, critical market and clearing and settlement processing occurred without major disruption. Some voice communications were affected, and those issues are being reviewed.

Overall, financial sector institutions' and crisis coordination groups' performance and activities were well-managed and well-coordinated among government and private sector entities. There is always room for continuous improvement, and lessons learned during these events are being acted upon. At the sector-level, we identified opportunities to further improve coordination related to disseminating information and communicating efficiently. For example, a more structured information flow among coordinating activities can minimize redundancy and facilitate timely receipt of information at all levels. Additionally, with multiple conference calls occurring to exchange information, a natural sequencing order could yield better situational awareness at regular intervals. Our sector council is examining these opportunities.

Summary

Chairwoman and Members of the Committee, we believe a strong public/private sector partnership is the right approach. The government and private sector's coordinating efforts during the recent power outage and storms demonstrated the preparedness work done by many organizations has yielded very positive results. These efforts help to further ensure our critical services will be resilient.

Treasury Secretary Snow noted the day following the power outage; "We applaud the initial response of critical financial institutions to the power outage. The men and women who make our markets work did an extraordinary job of ensuring that our financial markets lived up to their reputation as the most resilient in the world."

Thank you for this opportunity to testify.

About the Financial Services Sector Coordinating Council for Critical Information Protection and Homeland (CIP/HLS)

The Financial Services Sector Coordinating Council for CIP/HLS fosters and facilitates financial services sector-wide activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security. The council was created in June 2002, by the private sector, with recognition from the U.S. Treasury, to coordinate critical infrastructure and homeland security initiatives for the financial services industry. The five major areas of immediate focus for the council include: Effective and Rapid Information Dissemination; Crisis Management and Response Coordination; Outreach and Organizational Engagement; Knowledge Sharing and Best Practices and the National Strategies for Homeland and Cyber Security.

About Bank of America

One of the world's leading financial services companies, Bank of America is committed to making banking work for customers and clients like it never has before. Through innovative technologies and the ingenuity of its people, Bank of America provides individuals, small businesses and commercial, corporate and institutional clients across the United States and around the world new and better ways to manage their financial lives. The company enables customers to do their banking and investing whenever, wherever and however they choose through the nation's largest financial services network, including approximately 4,400 domestic offices and 13,000 ATMs, as well as 30 international offices serving clients in more than 150 countries, and an Internet Web site that provides online banking access to 4 million active users, more than any other bank.

For release on delivery
2:00 p.m. EDT
October 20, 2003

Statement of
Mark W. Olson
Member
Board of Governors of the Federal Reserve System
before the
Subcommittee on Oversight and Investigations
of the
Committee on Financial Services
U.S. House of Representatives

October 20, 2003

Introduction

Chairwoman Kelly, Ranking Member Gutierrez, and members of the Subcommittee, thank you for the opportunity to discuss the impact of the power outage experienced by several states on August 14 and 15, and the impact of Hurricane Isabel, which struck areas of the east coast--primarily the District of Columbia, Virginia, North Carolina and Maryland--on September 18 and 19. The Federal Reserve and the financial system, more generally, weathered the power outage with few difficulties and critical operations were largely unaffected. Markets and consumers remained calm. Hurricane Isabel did not have a noticeable effect on the operation of the financial system, although affected areas did experience a loss of power with collateral effects similar to the power outage.

Let me begin by emphasizing that it is no accident that the financial sector performed well in responding to the outages. Throughout its history, the banking industry has had many experiences with disruptions to normal business operations and has learned from experience the need to provide, maintain, and test appropriate backup facilities. This understanding has been enhanced by the preparations leading up to the year 2000 concerns about the resilience of our technology infrastructure and by the industry's response to the terrible tragedy of September 11, 2001. From these experiences, the industry has learned some lessons about providing sufficient backup for power and the likely collateral effects of experiences such as the recent outage. Moreover, because financial institutions rely on power to run mission critical information systems, events such as the power outage also underscore the need for institutions to integrate the risk of a wide-scale disruption into their enterprise-wide risk management strategies. Indeed, evaluating an institution's emergency preparedness is an important component of the Fed's bank examination procedures.

Impact on Financial Markets and Depository Institutions

The August 14 power outage occurred just after the close of most U.S. securities and futures markets. A rapid switch to backup power enabled market utilities to complete end-of-day processing and settlement activities without any material disruptions. Uncertainty was minimized when the markets announced early Thursday evening that they would open on Friday. With only one exception, the markets were able to open and close smoothly on Friday. Also, some financial institutions in Manhattan closed early on Friday to accommodate the limited availability of public transportation. Otherwise, the markets, clearing and settlement organizations and market participants were well prepared to operate on backup power at their offices or from more remote backup sites. In terms of market volatility, there was some limited--and understandable--volatility in energy-related futures contracts and securities prices on Friday.

The financial system did not experience any widespread or cascading liquidity dislocations, in large part because payment and settlement systems operated normally. The outage disrupted the federal funds market because most of the volume in that market typically takes place late in the day, and the market tightened considerably on Thursday afternoon. As a result, a small number of banking organizations had to turn to the Federal Reserve's discount window for overnight funds, and the Federal Reserve extended a larger volume of discount window loans on Thursday than is usual. The federal funds rate was volatile again on August 15, and borrowing remained somewhat elevated. Conditions in the federal funds market returned to normal after the weekend.

I note that, if the outage or collateral effects had rendered a Federal Reserve Bank inoperable, which it did not, the Federal Reserve has robust contingency arrangements in place under which another Federal Reserve Bank would have handled loan requests by depository institutions in the affected District.

Most depository institutions had backup power at their main offices, larger branches, data centers and operations facilities. As a result, the business of banking largely proceeded without interruption, although retail banking (taking deposits, making loans and dispensing cash) was disrupted at affected branch offices. It was also necessary to close some retail branches whose security monitoring systems were impacted by the outage in order to assure the security of cash, other assets, and personnel. Most ATMs in the affected areas stopped working, although a few had backup batteries that enabled them to function for a short period. Shortly after the power went out, the Comptroller of the Currency signed an order authorizing national banks, at their discretion, to close. Governors in a number of affected states made similar proclamations for state-chartered depository institutions. Probably not more than a few dozen depository institutions, predominantly small, regional and community organizations and foreign banking organizations, had to close all operations. In many instances, critical personnel spent Thursday night in their offices to assure continuity of operations on Friday. A number of organizations required only critical staff to report to the office on Friday due to limited availability of public transportation.

I must say that we are extremely proud that the financial markets and banking organizations were able to meet the various operational challenges of the outage without any systemic effects or loss of confidence in our financial system.

Impact on Consumer Confidence

The outage, which lasted less than 48 hours for most of the affected areas, had no discernable effects on consumer confidence. Consumers were patient and able to cope with the situation, including the temporary loss of access to local branches and ATM machines. There was no sense of panic and there were no unusual currency demands. We believe the public acted calmly in large part because the government was quickly able to determine and announce that the

outage was not an act of terrorism. Moreover, consumers have access to a broad range of retail financial services that are highly redundant and substitutable. For example, even though consumers could not withdraw cash from ATMs, they still could use checks. In many cases, they also were able to access bank call centers to effect transactions and obtain information. Electronic payments--deposits of paychecks and consumer transfers of money, such as mortgage payments--were not disrupted.

Impact on Federal Reserve Facilities and Operations

The Federal Reserve System has always placed a high priority on business continuity planning for its operations and services. The robust resilience that has been established was demonstrated during the August power outage and Hurricane Isabel. Throughout both of these recent events, the Federal Reserve was able to continue critical operations, provide services without interruption, and respond to market needs.

The August power outage affected Federal Reserve Bank offices in New York City; East Rutherford, New Jersey; Utica, New York; Cleveland; and Detroit. Despite the loss of utility power, these offices were able to continue operations without disruption using backup generators. Some of the affected offices heightened security as a precaution, but no incidents occurred. All Reserve Bank financial services operated normally during the outage, and for some services, the Reserve Banks extended their operating hours to meet the needs of depository institutions. For example, the Fedwire funds transfer service, our large dollar payment system, continued operations without interruption on the first day of the outage and opened on time the next day. The Fedwire funds transfer closing time was extended on both Thursday and Friday to accommodate Fedwire participants that were experiencing outage-related problems and late exchanges of fed funds. Similarly, the Fedwire securities service was unaffected on the first day of the power outage, and it opened normally the next day. The closing time for the securities

service was extended on Friday to accommodate participants affected by outage-related connectivity problems.

In general, although extensions of Fedwire closing times were required as a result of the power outage, there were no widespread problems among Fedwire participants. Most Fedwire participants in affected areas shifted quickly to backup power and were able to connect to Fedwire and continue processing transactions. A few participants, particularly some foreign banking organizations, experienced connectivity or processing problems. The Reserve Banks provided support to these organizations through their normal telephone-based, off-line processing service.

Federal Reserve Bank check processing centers in the affected areas operated on backup power, allowing check processing to proceed without interruption. The volume of check processing was slightly lower than normal on Thursday. Reserve Banks' inventories of currency were sufficient to meet depository institution demand during and after the outage. Consumers did not seek to withdraw unusually large amounts of cash during the outage--apparently continuing to use the normal mix of retail payment methods, including check and debit or credit cards at merchants that had backup power or were outside of the affected area. The Federal Reserve was not asked to provide currency outside of normal operating hours (after hours or weekend), but was prepared to provide extra cash shipments to depository institutions, if necessary. The Federal Reserve's Automated Clearinghouse retail electronic payment system was unaffected by the blackout.

There was no notable increase in the use of Federal Reserve intraday credit on the days of the power outage. Average System aggregate and peak intraday credit extensions were within reasonable levels. In addition, there was no notable increase in either the size or number of overnight overdrafts by banks across the Federal Reserve System.

Regarding the Board of Governors, we believe that a power failure in Washington, D.C., similar to the August outage, would have only a minimal impact on the Board. We recently completed upgrades to our backup electrical service to provide 100 percent of the power requirements for the Board's two main buildings. The Board also maintains adequate supplies of water to maintain operations. Priority contracts to deliver additional fuel and water are in place. By yearend, backup generators will be installed to provide hot water and heat in the event the Board's steam service is disrupted. In the event of a wide-scale power outage, our biggest challenge would be transportation. If the Metro or if traffic lights and street lights were out, it is likely that we would ask only emergency and critical staff to come to the Board's offices. Many of our professional staff can "dial-in" to the Board via their personal computers and work from home. In addition, the Board is reserving accommodations at hotels that have emergency power systems for Board members and our most senior staff to assure that they can get to the Board's offices in the event of a significant transportation disruption. Finally, the Board has established a number of business resumption and information technology backup sites within and well outside of Washington, D.C., that could be activated if necessary.

During Hurricane Isabel, the federal government was closed on Thursday, September 18, and Friday, September 19, to assure the safety of employees and accommodate the closure of public transportation systems. Emergency and critical employees were able to report to the Board during those days and over the weekend. Although much of the Washington, D.C., area lost power for as long as eight days, the Board was not affected and our critical business functions continued to operate.

Agency Coordination

The federal financial agencies have had a great deal of experience in coordinating their activities during various financial crises, natural disasters causing infrastructure disruptions, and

terrorist attacks. None of the agencies experienced operational problems from the outage. On Thursday afternoon, the agencies immediately activated crisis communication protocols. The Federal Banking Information Infrastructure Committee, made up of the federal and state financial regulators and a representative from the Homeland Security Council, held periodic conference calls throughout the day. The Federal Financial Institutions Examination Council, made up of the federal regulators of depository institutions, also held a series of calls regarding the status of supervised institutions. Each of the agencies followed internal crisis communication protocols across their organizations. As in the past, the ability of the agencies to share information and coordinate activities assured a consistent and cohesive response.

Lessons Learned

The Federal Reserve's and the financial sector's performance during the outage was very good, in part because power outages seem to occur periodically, and we have worked hard to prepare for them by establishing emergency backup power sources. However, lessons learned and opportunities for improvement flow from every event. The August outage is no exception.

One of the key lessons learned is that unexpected disruptions tend not to be limited to a firm's internal operations or facilities--the proverbial fire in the data center. In this era of unprecedented demand on the critical infrastructure and the increased threat of terrorist and cyber attacks, financial firms must plan how to recover critical operations and service customers in the event of a wide-scale disruption that affects a cross section of the industry as well as the critical infrastructure and the accessibility of key staff.

The importance of sharing timely and accurate information is a principle that is underscored every time we have an experience that disrupts any part of the nation's critical infrastructure and affects the public. This includes careful coordination of messages between federal and state authorities about steps being taken to protect the public and resolve the

problem. As I mentioned earlier, we believe that the government's announcement within hours after the event that the outage was not a terrorist act made a significant difference in how the public responded to the disruption. Similarly, Thursday's announcements that the New York Stock Exchange and NASDAQ were operating and would open on time on Friday did much to calm investors and markets here and around the globe. Financial firms and markets were forthright in advising stakeholders about their operational status and steps being taken to recover affected operations to meet customer needs.

Another area where we learned important lessons pertains to the adequacy of backup strategies for loss of power. For example, the sole use of batteries as backup proved wholly inadequate, particularly for aspects of the critical infrastructure, such as telecommunications switches. In most cases, banking organizations had provided for sufficient backup power to continue critical operations, such as payments, call centers, data processing and key management activities. Many had established backup power for key geographically dispersed retail branches. In other cases, firms learned that rented office space did not have anything more than emergency lighting for evacuation purposes. Others found that they had not provided backup power for in-house telecommunications systems, so while the telecommunications systems leading into and out of their building worked, their voice and data telecommunications systems did not. We understand that some key telecommunications facilities had not arranged for all of the critical functions at central office switch locations to have necessary backup power. We also learned that many cell phone towers are located on buildings that did not have emergency backup power. Some firms that were able to switch over to generators found it difficult to arrange for additional fuel because of transportation issues and because of competing demands and delivery priorities. This may suggest that the ability of some financial firms and the critical infrastructure to continue to provide backup power to critical operations might have degraded somewhat if the

outage had extended through the weekend and into the next business week. I would like to recognize the important efforts of the Office of Emergency Management for New York City in working closely with key critical infrastructure providers and market utilities to respond to unanticipated backup needs and manage transportation issues.

The power outage also emphasized the interdependencies across the critical infrastructure and the cascading impacts that occur when one component falters. The effects on transportation in Manhattan--with rapid transit systems down and rail stations closed in the city--prevented key staff at financial institutions from traveling to their offices and made it difficult to obtain fuel deliveries for generators. In Detroit and other cities, problems with water supplies necessitated the closure of buildings, even those with backup power. Access to potable water also was limited in a number of locations where pumping and sanitation stations did not have backup power or did not have sufficient backup power to operate at full capacity. The failure of steam generators in New York City caused a number of organizations to shut down. Most importantly, we saw a number of instances where telecommunications services were affected by insufficient backup power. Some of these instances were within the control of the affected financial firm, but many others were under the control of the telecommunications providers.

Conclusion

The lessons learned from the power outage emphasize the importance of preparing for a wide-scale disruption. They also emphasize the need for a sound and resilient critical infrastructure because of the significant collateral effects that can flow from a disruption in one component, in this case electric power. The Federal Reserve and the financial sector performed well during the outage. Nevertheless, we are encouraging financial firms and critical infrastructure providers to review their own lessons learned and, where appropriate, to take additional steps to achieve better resilience from the effects of a future power outage.

75

-10-

Thank you for the opportunity to discuss the effects of the power outage and Hurricane Isabel. I would be pleased to answer any questions you may have.

**TESTIMONY BEFORE
COMMITTEE ON FINANCIAL SERVICES
U. S. HOUSE OF REPRESENTATIVES**

**By Howard Schmidt
Vice President and Chief Information Security Officer
eBay Corporation**

Introduction

Chairwoman Kelly, members of the Committee, my name is Howard Schmidt. I am the Vice President and Chief Information Security Officer for eBay, where I lead a team responsible for ensuring the trustworthiness and security of the services that bring so many global citizens together each day. But, I come before you today primarily as an individual who has had the privilege of working with committed individuals in the private sector, law enforcement and government to forge the collaboration and cooperation that is so essential to safeguard cyber space. I assisted in the formation of some of the first collaborative efforts in the law enforcement community to address cyber crime in local law enforcement and the FBI and I helped lead the creation of the Information Technology Information Sharing and Analysis Center (IT-ASAC) and had the honor of serving as its first president. I also had the privilege of being appointed by the President to serve this great nation while leading, with Richard Clarke, the President's Critical Infrastructure Protection Board, which represented one part of the overall governmental response to the threat of cyber security attacks in the wake of September 11. I retired from 31 years of public service after completing and publishing the "National Strategy to Defend Cyberspace," working with a team of dedicated public servants, this body and the American public.

My remarks today will focus primarily on the transformation underway within both business and government to create the level of information sharing and collaboration necessary to safeguard computing and communications. The events of the late summer served to deepen our appreciation for the interdependency between the Internet and the critical infrastructure of commerce, as perfect storm emerged among the confluence of two major worms and viruses and the blackout.

This past year has again shown us dependencies we have on the various parts of the power and telecommunications infrastructure and how interrelated they both are. The power blackout of the Northeast this past summer was a unwelcome reminder of how inextricably the physical world and the "cyber" world are connected.

As if the power outage was not proof enough, the forces of nature again showed us the impact that a catastrophic event could have on our IT infrastructure and the systems they support.

In a public report by the North American Emergency Organization, they estimate that over 50% of businesses do not reopen their doors after a prolonged outage as we have seen this past year. Those that do face tremendous rebuilding cost as well as lost business.

One of the key things that help to reduce the impact of these disruptive events is the ability to share information, across sectors and across competitive lines. The same fundamental principals that have applied in cyber security information sharing apply in the cases of disasters as we have recently seen. During the events of this summer it is estimated that the online industry saw a 10-15% reduction of activity during the power outage and the hurricane. In a published report, a division of Eagle Rock Alliance outlined the financial impact of system failure by various industries and the estimated losses by hour based on system failures. In the financial services industry they cite that credit card/sales authorizations cost \$2.6 Million per hour, brokerage operations at a rate of \$6.45 Million per hour and home shopping \$113,000 per hour. As we can see by this report, the longer the duration of the event the more costly it becomes.

Although there is little we can do to stop a hurricane or other natural disasters we can do much to prepare for events such as these as insure the impact is of minimal duration by taking the same basic measures we would to prepare for a cyber security event. We must share best practices, identify threats and vulnerabilities and create an environment where information sharing becomes the rule, not the exception.

The use of increasingly sophisticated attack tools, with automated attacks penetrating the Internet in seconds, collaboration across industry and government is essential. The events of the late summer clearly highlighted the vulnerabilities and the challenges we face, but I also believe they illustrated the significant progress that has been made in creating an infrastructure for information sharing and collaboration.

Without committed companies working together and with government, I am convinced that the impacts of these events would have been far more severe. Recent initiatives by the Department of Homeland Security to implement the President's Strategy to Protect Cyber Space hold the potential to significantly enhance the momentum created by this increased collaboration. This will further reduce our risks to disruption of our critical infrastructure.

The Problem --- Building an Infrastructure for Cyber Security Protection Capable of Operating At Internet Speed

Today, the Internet connects over 170 million computers and an estimated 680 million users, with an estimated growth to 904 million by the end of 2004. From major data operations conducting large-scale financial transactions, to wireless devices keeping

families connected, the Internet touches virtually all aspects of our economy and quality of life. eBay is a prime example of how deeply ingrained the Internet is in American life. In one sense eBay offers an enhanced mechanism for transactions between buyers and sellers. More fundamentally, the success and popularity of eBay reflects the power of the Internet to extend and enhance the global marketplace.

More pointedly, the Internet has become a fundamental component of business processes--enhancing productivity by speeding connectivity between remote locations or across functional operations. The Internet is deeply ingrained in managing power, producing chemicals, designing and manufacturing cars, managing money and delivering government services ranging from human services to environmental permitting. The flip side of these productivity-enhancing applications is an increase in vulnerabilities.

The BLASTER and Sobig "worm" incidents and the blackout demonstrated the effect of these vulnerabilities. BLASTER and Sobig impacted operations ranging from major rail freight services to charter schools and local government operations. The impact of the blackout reached far beyond the affected region -- services such as home sale closings were delayed because of lost work days in major financial centers.

In assessing our ability to meet the challenges of these events and prevent their reoccurrence, it is essential to note that, in many ways, we have been racing to craft a infrastructure for cyber warning and response that is as dynamic as the Internet itself. Until very recently much of the formal governmental infrastructure for warning and response had changed little from the days when the Internet was used by a relatively small group of trusted users, sending generally non-confidential information to a small set of U.S. destinations very slowly. It was an infrastructure built to address attacks that took days to develop. This legacy warning and response network was still in part a vestige of a time when the private security industry was only in its infancy.

Today the Internet is utilized by hundreds of millions of users all across the globe sending information ranging from homework assignments and simple greetings to the most sensitive financial and operational data of government and industry, all at the speed of light. The Internet landscape also now includes a private sector security industry that has grown to an estimated \$17 billion per year in goods and services. And, as we are all painfully aware, attack speeds today are measured in seconds, not days.

The challenge is to craft a warning and response infrastructure that reflects the dynamics of today's Internet.

It must be an infrastructure that reaches across and engages the sectors and communities that utilize the Internet. It must harness, engage and empower the private security industry right at the heart of its operations. It must prove to be as nimble and flexible as those who attack the Internet. For example, as the focus of attacks shift in real time to particular categories of users, as we witnessed in BLASTER, the focus of our response must be capable of shifting.

The times also demand a response capability that can be a bridge between efforts to identify threats and vulnerabilities and build partnerships to reduce them ---much the way the treatment of symptoms of new biological viruses are synergistically and seamlessly connected to the resources committed to rapidly creating vaccines. In short, it must be faster, more collaborative and broader in its reach in order to shift the frontier from response and warning to prevention.

There will be no silver bullets in meeting these challenges. The creation of a dynamic warning and response infrastructure certainly involves new technologies that both speed response and, ultimately, protect systems from attacks. But the heart of the system will always be collaboration---real information sharing and coordination to identify, reduce and respond to threats and vulnerabilities within and across industries and with the government -- the very type of communication and information exchange that enabled some of our brightest minds in companies and response organizations to reverse engineer and mitigate the impact of the Sobig attack.

Emerging Solutions---Growing Collaboration in the Creation of a Cyber Security Infrastructure

Two of the earliest examples of private-public cooperation for “Cyber Crime/Cyber Security” were the formation of the High Tech Crime Investigators Association (HTCIA) and the Information Systems Security Association (ISSA). Both organizations date back to the mid/late 80’s and are dedicated to sharing of information on cyber crime and information security. They still exist today and their membership and value have increased significantly over the years.

The growth and evolution of private sector collaboration in information sharing, threat assessment, and incident mitigation has increased significantly by major private sector developments over the past few years: (1) Sector Coordinators; and (2) Information Sharing and Analysis Centers (ISACs), created by PDD 63 in 1998. These developments strike decisively at the issues of concern to this committee and continued progress in this area holds the greatest promise to secure cyber space.

Sector Coordinators: This is for each of the major sectors of our economy that are attractive to potential terrorist attack -- the federal government, designated lead agencies and DHS. A sector coordinator is an individual in the private sector identified by the sector lead agency to coordinate their sector, acting as an honest broker to organize and bring the sector together to work cooperatively on sector infrastructure protection issues. The sector coordinator can be an individual or an institution from a private entity. Sector coordinators may also identify a representative(s) at the working level for day-to-day activities.

These leaders provide the central conduit to the federal government for the information needed to develop an accurate understanding of what is going on throughout the nation’s infrastructures on a strategic level with regards to critical infrastructure protection

activities. The sector coordinators and the various sector members were key to the creation of the National Strategy to Defend Cyber Space.

Other functions of the sector coordinator include:

- Coordinate a national plan for infrastructure protection for its sector
- Facilitate outreach and awareness to support infrastructure protection plan implementation;
- Perform or coordinate risk assessment methodology and implementation for the sector, including interdependencies;
- Identify requirements for research and development necessary to meet the special needs of the sector;
- Help oversee the development of an information sharing mechanism (e.g., ISAC) for the sector, tailored to the special needs of the sector and infrastructure protection;
- Help develop or support requirements for sector wide guidelines/standards/useful/effective practices on infrastructure protection, training and education and implementation, metrics for success of infrastructure protection activities; and
- Identify and communicate obstacles or impediments to an effective infrastructure protection program that contains all elements of above;
- Serve as the coordination point for the sector's owners and operators in discussions with other sectors as needed (particularly to identify interdependencies, address common issues, and share effective practices); and
- Act as the coordination point of contact for the sector with the federal government at various infrastructure protection meetings, and the strategic communication point back into the sector and its members from the federal government.

Some sectors' diverse interests may make choosing a single sector coordinator challenging. Industry and the lead agency may explore innovative solutions, such as a coordination body or "virtual coordinator" based on existing networked resources, by designating separate sector coordinators to represent key sub-sectors who can, in turn, work together to represent the entire sector. The intention is for sector liaisons and coordinators to have a close working relationship and communication.

Second, of Information Sharing and Analysis Centers (ISAC): An ISAC is an operational mechanism to enable members to share information about vulnerabilities, threats, and incidents (cyber and physical). The sector coordinator develops these Centers with support from the sector liaison. In some cases, an ISAC Manager may be designated, who is responsible for the day-to-day operations of the ISAC, to work with the sector coordinator or the sector coordinating body with support from DHS and the lead federal agencies.

Presidential documents, such as the *National Strategy for Homeland Security*, continue to encourage information sharing and identify ISACs as an information-sharing model. Many of the ISACs, particularly since the events on September 11, 2001, incorporate more information on physical security.

An ISAC's purpose is to gather, analyze, and disseminate to its members an integrated view of information system and other infrastructure vulnerabilities, threats, and incidents that are relevant to the sector. An ISAC includes the following characteristics:

- 24 x 7 indications and warnings within the sector;
- Information sharing with government and other ISACs as desired;
- Receive alerts and warnings of threats and incidents for dissemination to sector from government and other sources;
- Receive vulnerabilities or remediation information for dissemination to sector from government and other sources; and

The information which ISACs commonly work with provide warnings, establish trends in types and severity of attacks, and share threats and solutions among the ISAC membership and other appropriate organizations, including the federal government.

Thus, Sector Coordinators and the ISACs essentially form a dynamic intersection among Internet users, vendors and public and private response communities.

Recent action taken by the Department of Homeland Security (DHS) to create the US CERT at Carnegie Mellon University has the potential to significantly enhance the continued growth and evolution of ISACs. The US CERT is designed to serve as a focal point for building partnerships based cyber security response network.

The goal for US CERT is to ensure that there is on average no less than a 30 minute response to any attack within one year. No surprises and faster response. The very specific nature of this goal is designed to deliberately focus the US CERT on building broad participation by ISACs and response organizations and the private sector.

The US CERT will undertake the following major initiatives:

- Develop common incident and vulnerability reporting protocols to accelerate information sharing across the public and private response communities.
- Develop initiatives to enhance and promote the development of response and warning technologies.
- Forge partnerships to improve incident prevention methods and technologies.

An immediate focus of the US CERT is to more fully engage and truly serve the ISACs--to ensure that they are right in the front lines of warning and incident communication. The new incident and vulnerability reporting protocols will include more responsive and

immediate engagement of the ISACs and the US CERT is designed to facilitate more immediate interaction with ISACs and among ISACs during major incidents.

FUTURE CHALLENGES

The creation of the US CERT will, for the first time link public and private response capabilities and facilitate communication on cyber security across all infrastructure sectors. Together with increased collaboration and coordination of cyber crime and forensics activities and the growth and evolution of Sector Coordinators and ISACs, the US CERT has the potential to create the national response network envisioned in the President's strategy.

But we can also be certain that as increased collaboration continues to enhance our protection and responsiveness, the nature and sophistication of attacks will also evolve. There are clear challenges we must address.

First, we must develop a clear strategy for the long-term growth and operation of the ISACs. No clear model exists for their long-term support. To what degree should these critical operations be privately financed? What degree of public support is appropriate given their essential role in safeguarding the lifeblood of our physical infrastructure? We must dedicate ourselves to addressing these growth issues immediately.

Second, we must renew our commitment to enhance consumer awareness of basic cyber security practices. The recent attacks demonstrate that home users can be an effective pathway to launch attacks. We need to build on the public/private initiatives to promote cyber security with a focused and aggressive outreach effort.

Third, while we build an effective response network we must not lose sight of the innovation frontier. Technologies on the horizon hold the potential to dramatically and potentially decisively transform our cyber security challenges. Self-healing computers, embedded technologies that enable devices to recognize and defend against attacks and devices which enhance both security and privacy are within reach of an aggressive technology development agenda. This effort must be industry led in collaboration with our best universities. Most importantly, it must be synergistically linked with our response initiatives.

Finally, we must recognize that cyber security is no longer merely about products, services and strategies to protect key operations. What is at stake in the effective implementation of advanced cyber security technologies and strategies is nothing less than the ability to unleash the next wave of information technology led growth in jobs and productivity. Cyber security is an essential enabler to the advent of the next generation Internet and all it holds for how we work live and learn.

I don't want to close without mentioning my expectation that many of these challenges will be addressed, and indeed met head-on, with tangible commitments and deliverables through the upcoming National Cyber Security Summit December 2 and 3. This Summit

will be co-hosted by the Information Technology Association of America, the U.S. Chamber of Commerce, TechNet and the Business Software Alliance, with the support of the Department of Homeland Security. I will have the honor to serve at that summit, as will many of the brightest minds and most innovative companies across all sectors of the economy.

The work of this summit won't take place over just the two days it is scheduled December 2 and 3, but through task force work programs that will drive toward solutions in intense work before during and beyond the Summit. We expect that many of these deliverable will be forwarded to DHS early next year, after which we can measure progress on an ongoing basis. We expect this to be an all-hands-on-deck effort where we bring together, distill and integrate many of the outstanding work products from many groups regarding cyber security metrics, software development and maintenance, public outreach initiatives, and, of course, public-private partnerships in information sharing and early warning systems.

Chairwoman, Kelly, this concludes my prepared remarks and I thank you for the opportunity to come before this committee and welcome any questions that you may have.



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

MARK W. OLSON
MEMBER OF THE BOARD

October 22, 2003

The Honorable Sue W. Kelly
Chairwoman
Subcommittee on Oversight and Investigations
Committee on Financial Services
House of Representatives
Washington, D.C. 20515

Dear Madam Chairwoman:

Thank you again for holding the hearing of your Subcommittee on the impact to financial institutions and financial markets of the Northeast power outage and Hurricane Isabel. In my testimony, I referred to the men and women of the Federal Reserve Board who worked on September 18 and September 19, 2003. Many of these employees spent the night of September 18 in the Board's buildings. Many other Federal Reserve employees also worked from home, on the road, or voluntarily reported to work during that period. The following group of employees was assigned the responsibility of ensuring that critical central bank functions would operate. In recognition of their performance during this critical period, I respectfully request their names be included in the permanent record of your Subcommittee's hearing.

Latonya Adams	Bobby Blyther	Jeanne S. Cousin
Exzyrodger M. Agonoy	Alfred L. Boggs	Grady E. Covington
William Anthony	Albert B. Bradford, Sr.	Geary L. Cunningham
Gary E. Bailey	James L. Briggs	Richard S. Dana
Nytisha A. Bailey	Norman D. Brooks	Thurman E. Davis
Tyrone L. Bailey	Debora C. Burford	Wendell O. Dean II
Moreese C. Barnes	Robert W. Burns	Earl Debrow
Adrian D. Barry	Angela M. Burroughs	William Dennison
Joel E. Batchelor	Dorothea P. Caldwell	David A. Dextrateur
Keith F. Bates	Samuel T. Campbell, Jr.	Earl A. DiLulio
JoeAnn Battle	Seth B. Carpenter	Futina Dixon
Richard L. Bayles	Aaron T. Carr	Kent D. Dixon
Donald Bell	Clarence C. Chamblee	Levy J. Dixon
Norman I. Bell	Ronald Clark	Rebecca S. Douglass
LaVern Bess	Maurice M. Cleveland	Larence D. Dublin
Steven P. Bezman	Nora E. Coaxum	Milton E. Dukes
Patrick S. Billingsley	Tyson L. Coble	Charles R. Ellison
Roosevelt Bluford	Thomas W. Coppersmith	Marianne M. Emerson

The Honorable Sue Kelly
Page Two

Shirley Evans	Michael S. Kobi	Keith M. Resar
Dennis E. Farley	Lyle S. Kumasaka	Alexander Roman
Mark E. Fleming	Donald M. Lambert	Raymond Romero
Leroy J. Flemmings	Edward A. Lavalle	Giovanna Carla Russo
Julius L. Frierson	James J. Lee	Thomas D. Sellew
Vincent Garcia	Gerard L. LeGrande	Bruce O. Shamberger
Stephen Gaston	Shawn C. Liu	John A. Shepherd, Jr.
Russell W. Givens	Theodore L. Lomax	Tommie Shropshire
Carolyn S. Glauser	Donald L. Lookabill	Donald A. Spicer
Tracey Glover	Alexander E. Mack	Debra A. Spratley
David P. Gomillion	Stephen R. Malphrus	Wallace Terry, Jr.
Vanessa A. Grandy	Harold G. Marable	Curtis M. Thomas, Sr.
Ralph Green	William T. Marcoux	Michelle V. Tillery-Fuller
Jeffrey J. Hallman	Floyd M. Matsuda	John D. Trent
Winthrop P. Hambley	Lola McConnaughey	Raymond E. Triggs
James M. Hancock	James R. McCoy	Crystal D. Trueheart
Maureen Hannan	Calvin Edward Milligan	Ronald Tucker, Sr.
Kwame Harps	Sharon L. Mowry	Kenneth Villareal
Dean Hatch	George R. Murphy	Jesse Villarreal
Herman E. Haynie	Louis G. Musgrove, Sr.	Willie A. Weddle
Dennis E. Hebb	Thomas O. O'Brien	Tina R. West
Jason B. Hertel	Charles F. O'Malley	Keith A. Wharton
Larry S. Hester	Carolyn B. Palmer	Irma J. P. White
Kevin R. Hill	Rodney C. Parker	William Whitesell
Robert A. Holmes	Justin M. Payton	Heather A. Wiggins
Eathen J. Hooks, Jr.	Anthony J. Perry	William Wiggins
Christopher M. Jennings	H. Fay Peters	Franklin W. Williams
John A. Jester	George H. Phillips, Jr.	Howard N. Williams
Lillian D. Johnson-Douglas	Justin O. Phillips	John R. Williams
Martin A. Jones	Samuel W. Plummer	Michael L. Williams
Marvin C. Jones	Thomas F. Pollaci	Tia M. Williams
Elmer Jordan, Jr.	Rhonda A. Powell-Butcher	Gerri E. Wilmer
Larry Kemper	Brian K. Preslopsky	Jeffrey A. Windsor
Richard B. Kennedy	John A. Price	Ivan K. Wun
Pokyoung Kim	Samuel D. Purnell	David W. Wyatt
Robert Louis King	Janet A. Ray	
Trudy A. Knight	Vicki A. Razick	

Thank you, Madam Chairwoman.

Sincerely,



Diana L. Taylor
New York State Banking Superintendent
Financial Services O&I Subcommittee
10/20/03

Thank you Members of the Committee.

I welcome the opportunity to submit this testimony on how the New York State Banking Department reacted to the blackout of August 14 and 15, which was bad, but could have been much worse, and to tell you something about how the Department prepared for emergencies.

As the regulator of financial institutions with more than \$2 trillion in assets and including some of the largest financial institutions in the nation and indeed the world, it is incumbent on the Department to be prepared to deal with any eventuality, be it an act of man or God.

Disaster planning is not a new field for the Department – as we rely heavily on electronic data and networking, one of our key lines of defense is drawn in cyberspace. Indeed, even before cyberspace existed, the Department has been concerned – some would say obsessed – with the sanctity of our systems.

And that is a good thing. Y2K may not have caused the widespread chaos that was so universally feared, but the phenomenon was good for one thing – it got us ready for the worst case scenario.

In part because of the procedures in place in the Department, our financial systems suffered no lasting ill effects after 9/11, in fact our systems and those of the banks are stronger for it, and fortunately, the blackout of 2003 was reduced to a blip on the radar screen, although an inconvenient one for many.

It could, of course, have been much worse. As it was, the blackout became a vehicle for testing our emergency procedures, and those of our regulated institutions. The result was very positive, allowing us to run through a real life scenario, and to expand our what-if analyses. It is impossible to plan for every eventuality, I don't think anyone expected a power outage that was so pervasive and so quick, but I want to commend our regulated institutions and our co-regulator the FRB for their responses. It is due to them that very little financial inconvenience was suffered by the public at large.

There was a certain amount of kismet in the timing of the power outage: by 4:11 pm, when the blackout hit New York, banking business was largely completed for the day, the equities and options markets had just closed and critical staff had not yet left for the day. If the power had gone down at a more inopportune time,

the challenges to business resumption and continuity would have been much greater, but still not insurmountable.

The blackout also showed that arbitrary geographical recommendations for back-up and recovery locations contained in the "White Paper" issued earlier this year, would not have been helpful in mitigating the effects power outage. Events showed that contingency plans must be flexible, keep in mind that adverse events can have region or nation wide effects, and that unexpected events will occur.

Our largest and most critical institutions all successfully implemented their back-up plans that enabled them to complete their daily transactions in a mostly routine way and shut down securely for the night. Furthermore, while the Banking Department obtained an Executive Order from the Governor declaring an emergency that would allow banks to close their doors if they needed to, or not open at all, very few institutions statewide availed themselves of that option.

Most closings were limited to branch offices and ATMs that were left without power, security and/or personnel. Some community banks, credit unions and foreign banking organizations were closed with minimal impact on the system. Despite these sporadic closings, no significant systemic or consumer issues arose.

For the Department itself, matters were slightly different.

In order for the Department to stay in business during an emergency such as the blackout that affected such a huge area, we need three things: power, telecommunications and people.

The Banking Department's headquarters at One State Street in lower Manhattan lost both power and communications ability. However, staff, equipped with Blackberry devices operating on a peer-to-peer basis (the computers and phones were down and cell phones were out of service), knew exactly what to do:

- Reached out to the State Emergency Management Office (SEMO) in the event they needed to deliver cash anywhere in the state or provide other services to affected communities or banking institutions and with the New York City Office of Emergency Management (OEM) to apprise them of the Department's situation.
- Monitored key New York State chartered institutions including the New York Clearinghouse, the Depository Trust Company, JP Morgan Chase, the Bank of New York and others to ascertain their individual situations and then proceeded to our fellow regulator, the Fed, to stay the night.

- Coordinated actions with our fellow regulators. Shared information on the status of the financial sector and provided input into the Financial and Banking Information Infrastructure Committee (FBIIC). FBIIC is a group of financial services regulators charged with improving coordination and communication among financial regulators and enhancing the resiliency of the financial sector. As a result of the Banking Department's participation with FBIIC during the blackout, the Department will be increasing its participation in on-going critical infrastructure projects.
- Assigned senior staff to the Federal Reserve Bank of New York to share information, coordinate responses to institutional and systemic needs and monitor institutions critical to the financial sector.

It is worthwhile noting that the Fed's facilities have the critical systems back up power, telecommunications and computer systems we needed during the outage to monitor our institutions for any event-related problems or breakdowns.

What if the situation had been worse? What if the power had not been restored the next day or the outage had somehow caused lasting damage?

Without giving away any secrets that could impinge on our ability to react appropriately in the event of a catastrophe, I want to lay out our Disaster Plan as it exists currently and then briefly mention some items about which we need to be particularly alert.

As I mentioned before, communication is key – many personnel carry Blackberry communicators at all times, as well as Department-issued cell phones. In addition, many examiners and all senior staff use laptop computers while off-site.

In the event of an emergency, the Department's toll-free Employee Emergency number is activated and a recorded message advises callers as to what actions they should take. Senior staff have at home and in the office, a copy of the Department's Contingency Plan Telephone Directory which enables them to initiate staff and institution phone trees to pass on critical information and instructions.

Alternatively, the Superintendent and senior staff have Satellite phones, GETS Enabled cell phones and GETS Card Access to ensure that they will be able to communicate with staff and each other should land lines be down or overwhelmed and regular cell phones inoperable.

Immediately after an event, it is our protocol to contact the Governor's office to assess the situation and to request an Executive Order declaring a bank emergency or holiday if necessary. The Department also coordinates with the

State Office of Emergency Management as a matter of course and sends personnel to the SEMO bunker if so instructed.

All other calls and contacts after that point are to our fellow regulators, including the FRBNY, FDIC, OCC and others, industry utilities and our banking institutions.

If it is necessary for the Department to operate offsite – that is, if the data center is not accessible for an extended period – be it days or weeks – we can be fully operational in a matter of hours at our hot site north of New York City.

This is possible because we back up all our critical systems everyday – NT servers, AS 400 and e-mail. The tapes are stored outside of New York City and can be delivered to the hot site within hours, if necessary.

I would like to take this opportunity to inform the Committee of one of many steps New York State is taking to address critical infrastructure needs of the financial sector.

Recognizing the financial sector's dependence on telecommunication networks and the lessons learned from the events of September 11, 2001, the New York State Public Service Commission (NYPSC) has begun a major study of network reliability.

In cooperation with NYPSC, the Banking Department has encouraged the active participation of the financial sector in this study. A white paper entitled "Network Reliability After 9/11", issued in November, 2002, assesses the current state of reliability, goals for the future and means of attaining those goals. NYPSC is now in the process of gathering comments on the white paper and I am encouraged to report that with some prompting from the Banking Department, six key financial sector participants in New York have agreed to participate in this process. Interested individuals can read document on the NYPSC's Website at www.dps.state.ny.us/DPS-NetworkReliabilityRpt.pdf.

This committee has also indicated an interest in our efforts with regard to cyber security. This is a key concern of ours: any institution, governmental or private sector can be attacked at any time via cyber channels. In response to the recent upsurge in viruses, worms and other malware, the Department has asked institutions under our supervision to increase their level of readiness to withstand cyber attacks.

As businesses that rely on customers' trust for success, financial institutions are very careful to avoid disruption of their services and to ensure that they have systems and controls in place designed to detect and prevent unauthorized intrusions.

In order to alert the industry to new attacks as they are discovered, we have asked all institutions under our supervision to report significant instances of computer viruses, worms, hacking attempts and web site defacements to the Department. Our request, which went out in the form of a letter, we also informed our institutions that we would share information with them on alerts and cyber incidents.

Since the letter was sent earlier this year, our banks and other financial services firms have not reported large-scale successful attacks although many banks tell us a number of hacking attempts occur on a regular basis. These attempts are generally unsuccessful and have not significantly increased. An increase in hacking attempts against a particular institution, sector, or region could be an indication of a concerted attack.

Information received is passed on to NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) without disclosing the name of the entity suffering the attack. We also share information with other regulatory agencies.

CSCIC has instituted a public-private partnership to meet the information security needs of this state. To give an example of how this works, this past Thursday, October 16, seven vulnerabilities identified in Microsoft Server and Windows were sent to the institutions we supervise. We believe that passing on these warnings is useful in warning smaller less sophisticated institutions of the threats and weaknesses that arise all too frequently and in letting all firms that we supervise know of the importance we place on cyber security.

In addition to our IT examination efforts, examiners conduct regular visits to banks supervised by the Department between regularly scheduled examinations. Other banks have examiners permanently assigned as Central Points of Contact. We have taken advantage of this presence to remind the financial community of the need for continued vigilance regarding information systems. Because the Department is sensitive to the level of regulatory burden on the firms under our supervision, we have incorporated an Information Assurance/Cyber Security component into the existing visitation and examination process.

The Department's examiners stress that information security is an enterprise-wide responsibility, not just a technology or security policy issue. It is a fundamental business issue, requiring effective management, oversight and accountability. Senior level involvement on an on-going basis is required. Security risks are ever evolving and may change quickly, requiring continual monitoring.

Information risk management is needed to mitigate risks. Security practices to reduce vulnerabilities and manage risk must be in place. Basic steps of a risk management program include: promoting awareness at all levels of the institution, assessment of information security risks, continuous monitoring and evaluation, and implementing policies, procedures, and controls to mitigate risks.

It should be stressed that "no one size fits all." Sound policies and practices should be implemented to reduce risk exposure. With risk-focused management, not all controls are called for in every situation. Adoption of controls should be guided by each institution's unique risk assessment and evaluation. There is a range of security options possible.

Simply making sure that recommended upgrades, security settings, and patches have been installed may prevent 80 percent or more of all attempted attacks. According to security professionals "security is a journey, not a destination". As threats evolve and hardware and software change, anti-virus software, firewall settings – technological solutions -- must be evolve to meet the new conditions.

In conclusion, the key to surviving a disaster with minimal and short term disruption is knowing what your role is, how to fill it and where to turn for help.

The financial sector has accomplished a great deal since 9/11 and has a lot of which to be proud. However, a great deal of work remains to be done. The Banking Department and the State of New York are committed to working with the industry and the federal government to do our part to address these critical issues.

Thank you.



**WRITTEN STATEMENT
OF
THE U.S. SECURITIES AND EXCHANGE COMMISSION**

**CONCERNING
THE PERFORMANCE OF THE SECURITIES MARKETS
DURING THE NORTHEAST POWER OUTAGE AND
HURRICANE ISABEL**

**BEFORE THE SUBCOMMITTEE ON OVERSIGHT
AND INVESTIGATIONS**

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

OCTOBER 20, 2003

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

**WRITTEN STATEMENT OF
THE U.S. SECURITIES AND EXCHANGE COMMISSION
CONCERNING THE PERFORMANCE OF THE SECURITIES
MARKETS DURING THE NORTHEAST POWER OUTAGE
AND HURRICANE ISABEL
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON FINANCIAL SERVICES,
UNITED STATES HOUSE OF REPRESENTATIVES**

OCTOBER 20, 2003

Chairwoman Kelly, Ranking Member Gutierrez, and Members of the Subcommittee:

The Securities and Exchange Commission ("SEC" or "Commission") is pleased to submit this statement concerning the performance of the securities markets during the northeast power outage on August 14-15, 2003. Overall, it appears that most of the markets, clearing organizations, and other critical market participants within the areas affected by the August power failure operated remarkably well under these trying conditions. The extensive business continuity planning that these organizations have conducted under the Commission's oversight over the last ten years provided them with the requisite expert personnel, backup systems, and procedures to operate through the grid failure and overcome unanticipated byproducts of the electrical outage. Moreover, while Hurricane Isabel did not significantly affect the financial markets, the precautions that were taken in anticipation of this event serve to illustrate the contingency planning and emergency management efforts that the Commission undertakes with the securities markets and supporting organizations to address the myriad types of threats that might disrupt the orderly operation of the markets.

THE COMMISSION'S INITIATIVES IN BUSINESS CONTINUITY PLANNING

As the agency chiefly responsible for the nation's securities markets, the Commission has established a number of programs to improve the resiliency of this critical financial sector. For example, in the early 1990s, the Commission established its Automation Review Policy ("ARP") and a cadre of specialized staff to review the capacity and resiliency of the securities markets and clearing organizations.¹ The Commission's ARP staff inspects the information technology systems of these entities and controls over those systems, participates in periodic comprehensive evaluations of these systems, and issues recommendations for improvements in these programs as necessary. Moreover, the Commission has worked extensively with the markets and clearing organizations since the tragic events of September 11th to improve their capacity to withstand wide-scale disruptions. These efforts have included fostering the development of backup data centers and trading floors, as well as agreements between markets to serve as backup

¹ In anticipation of the Year 2000 conversion, the Commission's ARP program was subsequently extended to electronic trading systems known as Electronic Communication Networks ("ECNs").

trading venues for each other's securities if events warrant. The Commission has also worked with other regulators to establish best practices guidelines to strengthen the resilience of core clearance and settlement organizations.² The SEC has supplemented these efforts by issuing a Policy Statement that sets forth certain basic principles of business continuity planning, including a next-day resumption goal, that should be applied by the trading markets.³ The SEC staff intends to engage in an ongoing and individualized dialogue with each equity securities trading market, including ECNs, to discuss application of these principles in a manner most appropriate for the particular trading market.

THE NORTHEAST POWER GRID FAILURE

The Commission carefully monitored developments throughout the northeast power grid failure on August 14-15, 2003. As part of this effort, the staff consulted repeatedly with officials at the securities markets and clearing organizations within the affected areas in the greater New York metropolitan region. In addition, the staff conducted a series of conference calls during the outage that provided opportunities for markets and clearing organizations outside of New York to hear directly from the affected organizations concerning how they were coping with the power failure and how they planned to operate under these conditions. Moreover, the Commission staff participated in a number of calls with other financial regulators within the interagency working group known as the Financial and Banking Information Infrastructure Committee ("FBIIC") in order to keep them apprised of how the power outage was affecting critical markets and market participants.

² The SEC, together with the Federal Reserve and the Office of the Comptroller of the Currency, recently published an *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, SEC Release No. 34-47638 (April 7, 2003) ("Interagency Paper") that identified "sound practices" relating to business continuity planning for certain key market participants. The goal of this project was to minimize the immediate systemic effects of a wide-scale disruption by assuring that the key payment and settlement systems could resume operation promptly following a wide-scale disaster, and major participants in those systems could recover sufficiently to complete pending transactions. In this way, market participants unaffected by the disaster could continue to operate with minimal disruption and, when those impacted by the event were in a position to resume operations, the critical infrastructure would be available for them to do so. The sound practices identified by the Interagency Paper include: (1) intraday resumption or recovery goals; (2) maintenance of sufficient geographically dispersed resources to meet those goals; and (3) routine testing of business continuity arrangements. The Interagency Paper, however, focuses only on the key payment and settlement systems, and does not address the resilience of the trading markets.

³ SEC Release No. 34-48545 (September 26, 2003).

1. Major Equity Markets Performed Well

The power grid failure began to affect New York City at approximately 4:11 p.m. on Thursday, August 14, 2003.⁴ By this time, the vast majority of trading in the stock and options markets had already ended,⁵ and New York-based markets reported that their back-up electrical power enabled them to conduct an orderly shut down of their systems so as to preserve essential trading data. Moreover, New York-based clearing organizations reported that their back-up power capacity permitted these entities and their clearing firms to successfully complete the critical processing that occurs after the trading day (clearing trades, settling trades, transferring securities and funds, etc.).

Later on Thursday evening, the two largest U.S. stock markets, the New York Stock Exchange (“NYSE”) and the Nasdaq Stock Market (“Nasdaq”), announced their intention to open for trading the next morning. Overnight on Thursday, the NYSE prepared for the next day’s trading by using power from batteries and generators at its Wall Street trading floor.⁶ By the 9:30 a.m. market opening, however, the Wall Street trading floor was able to convert back to utility power, which was maintained throughout the Friday trading session. Nasdaq’s operational center operated on generators until 11:00 p.m. on Thursday, but was back on utility power afterwards and throughout Friday’s session. Utility power at Nasdaq’s backup center was not interrupted. Both the NYSE and Nasdaq were able to operate regular trading hours on Friday. In addition, the International Securities Exchange (“ISE”), a New York-based electronic options exchange, was able to trade normal hours on Friday using generator power. Moreover, several active ECNs located in the New York area also were able to operate normal hours on Friday using batteries, generators, or utility power.

The American Stock Exchange (“Amex”), however, experienced an unanticipated byproduct of the electrical grid failure that prevented the exchange from operating as planned on Friday. Over Thursday night, the Amex prepared to open on Friday using generators for its electronic systems. At around 2:00 a.m. on Friday, however, there reportedly was a sharp drop off in the steam feeds generated by Consolidated Edison that the Amex uses for the cooling system that is needed for the electronics on the exchange’s trading floor.⁷ While the Amex’s off-site back-up trading floor had adequate generator

⁴ All times are Eastern.

⁵ The regular trading session for stocks closes at 4:00 p.m., while the trading session for equity options closes at 4:02 p.m. The trading sessions for stock index options and most exchange-traded funds (“ETFs”) close at 4:15 p.m. In addition, after-hours trading in stocks continues after 4:00 p.m. on Nasdaq and a number of exchanges and ECNs, although after-hours trading volume rarely accounts for more than 3% of total daily share volume in stocks. There were no reported problems in post-4:11 p.m. trades in any of these securities on Thursday.

⁶ The NYSE’s backup trading floor also had generator capacity in case this facility was needed.

⁷ The Amex indicated that the Consolidated Edison steam system never failed before, including during the massive power outages in the 1960s and 1970s and on September 11, 2001. In view of the events during the August 2003 blackout, however, the Amex will be working with the SEC to

and cooling capacity to operate, exchange officials determined that there was not adequate time to fully activate this floor and relocate key personnel to this site on Friday. As a result, Amex officials decided instead to obtain a back-up steam-generation boiler to support its main trading floor even if this required a delay in its trading session. The Amex apprised the SEC staff of this determination early on Friday morning⁸ and the staff briefed the FBIIC agencies on this situation immediately thereafter.⁹ The Amex was able to obtain a back-up steam-generation boiler with the assistance of the New York City Office of Emergency Management (“OEM”). This boiler was installed at noon and the Amex began accepting orders in its stocks, ETFs, and options at 3:45 p.m. for closing rotations in these securities from 3:55 p.m. until 4:15 p.m.

Another unanticipated byproduct of the power outage involved deteriorations in the reliability of telecommunications within the affected areas. As was evidenced on September 11, 2001, impaired telecommunications can severely interfere with the orderly operation of the securities markets.¹⁰ Although the telecommunication problems experienced during the power outage were not nearly as prolonged or widespread as those following the events of September 11th, the sporadic cell and landline telecommunications interruptions on August 14-15 did adversely affect some efforts to ensure that normal trading operations could resume. For example, some firms reported that problems with cell phone communications interfered with efforts of their disaster recovery teams to coordinate effectively with some of their key personnel who were scattered over New York on the evening of August 14. In addition, even on the following morning, a regional exchange outside of New York reported that problems at a landline telecommunications vendor appeared to interfere with its intermarket trading system linkage to the NYSE. Moreover, one of the larger ECNs based in New York indicated that problems at another landline telecommunications vendor disrupted some of the voice lines that supported trading. Other broker-dealers also reported intermittent telecommunications problems. Nevertheless, we are pleased to be able to report that the affected institutions indicated that they were able to resolve their problems through workarounds or by contacting their telecommunication service providers.

As on Thursday, all of Friday’s after-market trade processing occurred essentially without incident. One of the institutions handling the bulk of securities clearing and settlement chose to handle those operations from one of its alternate sites, although it

determine what additional measures should be taken to improve the resilience of the exchange’s cooling capacity.

⁸ The New York City Office of Emergency Management joined the SEC and the Amex in a 7:00 a.m. conference call that included a discussion of the Amex’s need for a backup steam-generation boiler.

⁹ The Amex issued a press release at approximately 9:25 a.m. to announce its plans for a delayed opening.

¹⁰ The four-day closure of the stock market following the September 11th terrorist attacks resulted primarily from access limitations and telecommunications outages in the New York financial district following the collapse of the World Trade Center towers.

reports that it could have handled the operations from its primary facility if this had been necessary.¹¹

2. The Bond Market Also Performed Well

The bond market, like the equity markets, performed relatively well during the power outage. When the power went out at 4:11 p.m., the bond market was still open. (It is essentially always open.) There was an initial burst in trading volume and an initial spike in prices, but that subsided as it began to appear that the outage was not a terrorist act and as bond traders evacuated their trading desks in New York. As with equities, there were no reported losses of trading data, and the trade processing functions (clearing, settlement, transfer) went well. During this trading, bond markets also relied on back-up power systems.

As with equities, by 6:00 p.m. on Thursday, the Bond Market Association announced that New York-based bond trading desks would be open for trading the next day, Friday. New York-based bond trading desks did, in fact, open for trading on Friday as planned. Later in the day, however, the Bond Market Association recommended that bond firms should close their trading operations early in order to permit New York-based personnel to leave early (at that time New York mass transit was still not functioning). While the bond market technically stayed open, most New York-based bond trading desks closed for the day at 2:00 p.m. As on Thursday, end-of-day trade processing went well.

Although there were no major problems in the bond market, some participants did report problems with their telecommunications. For example, some trading desks reported problems with their telecommunications connections to information services that provide real-time market data.

HURRICANE ISABEL

While Hurricane Isabel largely bypassed major financial centers such as New York on September 18-19, 2003, extensive preparations were undertaken by both private and governmental organizations to prepare for potential problems that this storm might cause.

- By Monday, September 15, Hurricane Isabel was reported to have winds of 155 miles-per-hour (making it a severe Category 4 storm) and its track indicated that it would likely hit the U.S. East Coast later that week. Accordingly, the Commission staff engaged in a number of contingency planning efforts with the markets, clearing organizations, and the securities industry, as well as with other government officials in Washington, D.C., and New York City.¹²

¹¹ In order to guard against further disruptions, this institution's primary and back-up sites maintained generator power throughout Friday, even when utility power became available.

¹² The SEC staff had been briefed by OEM officials at a FEMA conference in July 2003 on the potentially severe impact that a Category 4 hurricane could have on New York City.

- On September 15, the SEC staff contacted officials at clearing organizations to ensure that they were prepared to respond to the possibility that Hurricane Isabel might force the closure of the equity markets on September 19, which would be an Expiration Friday for options and futures. The clearing officials confirmed that adequate procedures were in place to address this possibility.
- The SEC staff also checked with officials at the New York City OEM and local FEMA regional office concerning their contingency planning for the hurricane. Officials at OEM indicated that they were scheduling a planning meeting the next day at their Emergency Operations Center. This meeting would include representatives from the Securities Industry Association (“SIA”),¹³ and the SEC staff notified officials at the New York City exchanges and clearing organizations so that they could also send representatives to this planning meeting. Staff members in the SEC’s New York regional office also were designated to attend this meeting.
- On Tuesday, September 16, the OEM planning meeting went over how city officials were likely to respond to “worst case” scenarios involving Hurricane Isabel. OEM officials later briefed SEC staff members in Washington, D.C. on the issues discussed at this meeting. In addition, because the latest storm track indicated that the Mid-Atlantic coast was likely to receive the brunt of the hurricane, SEC staff checked with officials at the Philadelphia Stock Exchange and the Maryland operations center for the NASD to ensure that their organizations had taken the necessary precautionary measures. The SEC staff also confirmed with the Amex that its back-up steam-generation boiler and electrical generators were in place.
- On Thursday, September 18, the SEC began to staff its MarketWatch monitoring center on a 24-hour basis.¹⁴ Officials at the markets, clearing organizations, OEM, SIA, and FBIIC were notified that MarketWatch staff would be available throughout Thursday and Friday for emergency communications even though the local federal government offices were closed. MarketWatch operations were maintained over Thursday night in case the storm track changed to hit the New York area directly and the markets had to decide whether to open the next day.
- As Hurricane Isabel moved through the Mid-Atlantic region on Thursday and Friday, there was relatively little impact on the securities markets. The NASD

¹³ The SIA normally has representatives in place in the New York City Emergency Operations Center whenever it is activated.

¹⁴ The SEC’s MarketWatch center has back-up electrical power from batteries and generators and has redundant market-monitoring and news-retrieval systems (including television feeds over both cable and satellite). The center also has redundant communication systems to connect the SEC with markets, clearing organizations, and other regulators in emergencies. Moreover, the SEC has established an off-site back-up MarketWatch center that operates on other power grids and also has back-up power capabilities.

operations centers did have to operate on backup electrical power on Friday, but other markets and clearing organizations operated normally throughout the day.

Overall, therefore, Hurricane Isabel did not significantly affect the securities markets. Nevertheless, these events served to illustrate once again the importance of the public and private sectors to effectively coordinate their contingency planning efforts to address potential threats to the infrastructure of the financial markets.

CONCLUSION

The ability of the nation's securities markets to operate through the August power outage and the preparations undertaken for Hurricane Isabel serve as testament to the long-standing efforts of exchanges, clearing organizations, and other key market participants to improve the resiliency of their critical operations. Moreover, when unanticipated problems arose as byproducts of the electrical grid failure, the organizations' disaster recovery teams were able to work through these problems to restore essential systems. Nevertheless, problems such as those experienced in telecommunication systems during the power outage serve as a reminder of the critical role these systems play in the orderly operation of the markets and the need to further strengthen their ability to withstand wide-scale disruptions.