FINANCIAL SERVICES SECTOR PREPAREDNESS

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, FINANCE, AND ACCOUNTABILITY

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

SEPTEMBER 26, 2005

Serial No. 109–124

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

26–505 PDF WASHINGTON : 2006

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

CONTENTS

FINANCIAL SERVICES SECTOR PREPAREDNESS

SEPTEMBER 26, 2005

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
FINANCE, AND ACCOUNTABILITY,
COMMITTEE ON GOVERNMENT REFORM,
Brooklyn, NY.

The subcommittee met, pursuant to notice, at 10:07 a.m., at the Brooklyn Law School, 250 Joralemon Street, Brooklyn, NY, Hon. Todd Russell Platts (chairman of the subcommittee) presiding.

Present: Representatives Platts and Towns.

Staff present: Michael Hettinger, staff director; Tabetha Mueller, professional staff member; Daniel Daly, counsel; and Adam Bordes, minority professional staff member.

Mr. PLATTS. A quorum being present, this hearing of the Committee on Government Reform Subcommittee on Government Management, Finance, and Accountability will come to order.

I'd like to thank first the Brooklyn School of Law and my esteemed colleague and ranking member of our subcommittee, Mr. Towns, for hosting this field hearing here in Brooklyn. We're here in New York because this is the heart of our Nation's financial sector. On September 11, 2001, terrorists destroyed the World Trade Center in an attempt not just to murder and maim, but to dismantle our economy. With the backdrop of two destructive hurricanes, we see that any disaster, whether natural or man made, requires us to be well prepared. This hearing is about the preparedness of the financial sector in particular.

The rapid recovery of the financial infrastructure after September 11th inspired confidence throughout America. The U.S. Treasury securities market opened just 2 days later and the equities market was in full operation by September 17th. Still, Congress, the executive branch and industry realized that financial firms would need new contingency plans. The Federal Government in partnership with local governments and the private sector responded with a variety of initiatives. Many of these post September 11th improvements were tested during the massive power blackout on August 14, 2003. All indications after the blackout were that improvements put in place after September 11th helped mitigate the damage that could have resulted from the infrastructure shutdown and panic the blackout caused. These results are encouraging.

The purpose of this hearing is to examine the present status of financial market preparedness for wide scale disasters or disruptions, including efforts aimed at prevention, detection and re-

sponse. This hearing will provide local, State and Federal Government officials and representatives from the private sector a chance to discuss accomplishments and identify areas where improvements and resources are still needed.

[The prepared statement of Hon. Todd Russell Platts follows:]

COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, FINANCE AND ACCOUNTABILITY

OVERSIGHT FIELD HEARING:

FINANCIAL SECTOR PREPAREDNESS IN A POST-9/11 WORLD

OPENING STATEMENT OF
CHAIRMAN TODD RUSSELL PLATTS
SEPTEMBER 26, 2005

I would like to thank the Brooklyn School of Law and my esteemed colleague and Ranking Member of our Subcommittee, Ed Towns, for hosting this field hearing. We are here in New York because this is the heart of our nation's financial sector. On September 11, 2001, terrorists destroyed the World Trade Center in an attempt not just to murder and maim, but to dismantle our economy. With the backdrop of two destructive hurricanes, we see that any disaster – whether natural or man-made – requires us to be prepared. This hearing is about the preparedness of the financial sector in particular.

The rapid recovery of the financial infrastructure after 9/11 inspired confidence. The U.S. Treasury securities market opened just two days later, and the equities market was in full operation by September 17th. Still, Congress, the executive branch, and industry groups realized that financial firms would need new contingency plans. The Federal government in partnership with local governments and the private sector responded with a variety of initiatives.

Many of these post 9/11 improvements were tested during the massive power blackout on August 14, 2003. All indications after the blackout were that improvements put in place after 9/11 helped mitigate the damage that could have resulted from the infrastructure shutdown and panic that the blackout caused. These results are encouraging.

The purpose of this hearing is to examine the present status of financial market preparedness for wide-scale disasters or disruptions, including efforts aimed at prevention, detection, and response. The hearing will provide local, State, and Federal government officials and representatives from the private sector a chance to discuss accomplishments and identify areas where improvements and resources are still needed.

We have a very distinguished group of witnesses, beginning with **Mr. Raymond W. Kelly,** Police Commissioner, for the City of New York. Commissioner Kelly will be followed by **Mr. D. Scott Parsons,** Deputy Assistant Secretary for Critical Infrastructure Protection and Compliance Policy from the U.S. Department of the Treasury, **Mr. R. James Caverly,** Director of the Infrastructure Coordination Division at the U.S. Department of Homeland Security, and **Mr. Daniel A. Muccia,** First Deputy Superintendent of Banks from the State of New York Banking Department.

On our third panel will be **Ms. Catherine Allen,** Chief Executive Officer of BITS, The Financial Services Roundtable, and **Mr. Donald Donahue,** Chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, **Mr. Samuel Gaer,** Chief Information Officer for the New York Mercantile Exchange, **Mr. Steve Randich,** Executive Vice President of Operations and Technology and Chief Information Officer for The NASDAQ Stock Market, Inc. We look forward to your testimony.

Mr. PLATTS. We have a very distinguished group of witnesses, beginning with Mr. Raymond W. Kelly, police commissioner for the city of New York. Commissioner Kelly, thanks for being with us.

Mr. KELLY. Thank you, sir.

Mr. PLATTS. Commissioner Kelly will be followed by Mr. D. Scott Parsons, Deputy Assistant Secretary for Critical Infrastructure Protection and Compliance Policy from the U.S. Department of Treasury; Mr. R. James Caverly, Director of the Infrastructure Coordination Division at the U.S. Department of Homeland Security and Mr. Daniel A. Muccia, first deputy superintendent of banks from the State of New York Banking Department.

On our third panel will be Ms. Katherine Allen, chief executive officer of BITS, the Financial Services Roundtable and Mr. Donald Donahue, chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security; Mr. Samuel Gaer, chief information officer for the New York Mercantile Exchange; Mr. Steve Randich, executive vice president of operations and technology and chief information officer for the NASDAQ stock market.

Thank you again all for being here today and we look forward to your testimony.

I'm pleased now to yield to our ranking member, the gentleman from New York, Mr. Towns, for purposes of an opening statement.

Mr. TOWNS. Thank you very much, Mr. Chairman. Thank you for holding this hearing today in Brooklyn. I'd also like to thank our police commissioner, Mr. Kelly, which I'd say is the finest commissioner this city has ever known or seen. He's done a fantastic job over the years. Always a pleasure to see you here.

Mr. KELLY. Thank you, sir.

Mr. TOWNS. I'm pleased to welcome our Government Management Subcommittee to our home town, Brooklyn, NY, New York and look forward to our distinguished panel from both the public and private sectors. The financial capital of the world, New York remains a vital component of economic growth, both domestically and abroad. Although political and economic alterations have shaped and changed the marketplace in recent years, banks, brokers, government lenders and Wall Street have remained the backbone of our capital and currency markets from Brooklyn to Beijing.

The New York Stock Exchange alone accounts for approximately 2,800 companies with a combined market capitalization of nearly $20 trillion. On an average day the New York Stock Exchange trades nearly 1½ billion shares for an average daily dollar volume of roughly $50 billion. Stock and equity instruments, however, are not the only source of economic reliability for our markets. Future commodities and options trading at places such as the New York Mercantile Exchange serve as a major investment vehicle among institutional investors, pension funds and economic forecasters for domestic and foreign companies. Imagine the crisis our domestic manufacturers or agricultural sectors would be faced with if they did not have access to a viable commodities trading platform for energy products.

Recent events, however, beginning with the tragedy of September 11, 2001 have forced both government and industry at all levels to reevaluate how well we are prepared to maintain stability and con-

tinuity in the marketplace should another disaster occur. Such events are not only fiscal in nature, as electronic attacks on our electricity and telecommunication grids can prove as consequential and costly as a physical attack.

The government and private sector have appropriately embraced the need for stronger planning and coordination of activity since September 11th and have successfully begun to incorporate risk-based activities in their plans to reduce the threats facing industry and the physical infrastructure, human capital and personnel and information sharing capabilities. Backup systems and fiscal entities separate from current operations are now common among brokerage houses and trading platforms. Nevertheless, the various types of threats facing our financial services sector require planning at not only the Federal level, but at the State and local levels of government as well.

While the Department of Homeland Security may coordinate information sharing activities and threat level analysis, it would require the Metropolitan Transportation Authority, the New York PD and the Office of Emergency Management to execute a broad-based evacuation of Wall Street or southern Manhattan in the event of a physical attack within the surrounding area. These activities would require State authorities to reconfigure travel patterns on interstate highways and area bridges to insure safety and orderly evacuation activities. Furthermore, the functionality and reliability of our telecommunication electricity and pipeline grids will require both Federal and State coordination of activities in order to remedy and preserve the security of our energy resources in the wake of a disaster.

From this perspective, I hope our witnesses can demonstrate for us a clear delineation of responsibilities among both government and regulators and private sector participants. An underlying tenet of our market-based model is the level of trust and transparency investors both large and small can place in our institutions. It is our responsibility for planning and executing an adequate level of security and reliability for market activities that is shared at all levels of government in concert with private sector participants.

Thus, I hope our witnesses will speak to this blueprint of coordination, execution and transparency to insure that our market remains the bedrock of economic growth for centuries to come.

Again, I'd like to thank all the witnesses for appearing today, and on that note, Mr. Chairman, I yield back.

Mr. PLATTS. Thank you, Mr. Towns. We'll commence with the testimony of Commissioner Kelly. If you don't mind, would you please stand and be sworn in?

[Witness sworn.]

Mr. PLATTS. We'll note that the Commissioner affirmed the oath in the positive. We'll proceed, we have a general guideline of about 5 minutes, but, Commissioner, we're delighted to have you here and the expertise you have, he may be giving you some guidance on time, but we really would like to you take whatever time you need to share your insights with us.

STATEMENT OF RAYMOND KELLY, POLICE COMMISSIONER, CITY OF NEW YORK

Mr. KELLY. Thank you very much, Mr. Chairman and Congressman Towns. Good morning and thank you for inviting me today.

Defending this city, the financial capital of the world, from a terrorist attack is the No. 1 priority of the New York City Police Department. Accordingly, I'd like to focus my remarks today on the preventive measures the department is taking against this threat.

As you know, one of the stated aims of Osama Bin Ladin and al-Qaeda is to target America's economy. Shortly after the September 11th attacks, bin Laden himself exulted in the massive blows suffered by the U.S. economy, offering in an interview his own estimation of over $1 trillion in losses. We have no doubt that he seeks to replicate that strike if possible.

Since then, we learned of another plan to target financial institutions in New York. This after authorities discovered detailed surveillance of the Stock Exchange and the Citigroup Center in the laptop computer of an al-Qaeda operative captured in Pakistan last year. This followed two additional al-Qaeda plots to target the city in 2003; the first to bring down the Brooklyn Bridge and the second to smuggle weapons through a garment district business into the heart of Manhattan. These plots were foiled by increased police visibility and good intelligence sharing.

I cite them as evidence that New York City remains squarely in the cross hairs. Consequently, nowhere else is the effort to prevent another attack being undertaken with greater urgency. In addition to the dollar cost, this has required that we divert 1,000 police officers to counter-terrorism duties every day, and engage in extensive training and preparation. We've also undertaken a range of defensive measures to protect and harden the downtown financial district and enlist the support of the private sector.

Beginning in January 2002, we created a new bureau of counter-terrorism and we restructured our intelligence division. We've recruited outstanding individuals with extensive Federal intelligence and counter-terrorism experience to run them. We expanded our presence on the Joint Terrorist Task Force with the FBI and we posted detectives to seven other countries to enhance the flow of information we receive about any threats relevant to New York City.

We established one of the premier counter-terrorism training centers in the Nation right here in Brooklyn. In addition to our own core of 37,000 police officers, we have delivered training through that center to the members of the New York City Fire Department, the Metropolitan Transportation Authority Police Department, New York State Police; Nassau, Suffolk, Westchester, Rockland County Police and other agencies. We have also brought in dozens of private security professionals from hotels, banks and other institutions and trained them to better protect their facilities. Through our Nexus program we are reaching out to businesses that terrorists might seek to exploit. We want businesses to report any unusual order or anomalies that might suggest terrorist involvement. Detectives have paid thousands of visits to businesses throughout the city to increase their counter-terrorism awareness.

In July we launched a new initiative with the private security industry in New York called NYPD Shield. We are establishing a se-

cure Web site with training materials and threat information updates and we have offered detailed briefings on topics such as the London bombing and the attacks on the Egyptian resorts at Sharm el Sheikh. We also exchange threat information daily with the city's corporate and institutional security directors through an instant messaging system.

We have expanded the protection of critical infrastructure throughout the region. We have created the threat reduction and infrastructure protection program [TRIPS]. We've also divided critical infrastructure into five categories and assigned a team of detectives to cover each one. These investigators visit facilities throughout the city, identifying vulnerabilities and developing comprehensive protection plans with site managers to prevent attacks.

In 2003, at the beginning of the war in Iraq, we implemented a comprehensive security plan known as Operation Atlas. Given the ongoing terrorist threat Atlas remains in effect today. Broadly speaking, Operation Atlas has tightened the protective net around the city by increasing vigilance at entry points into New York and by placing mass transit and other potential targets under much greater scrutiny.

Turning to the financial district itself, beginning in 2002, the Police Department engaged in extensive collaboration with the New York Stock Exchange and downtown business leaders to harden the financial district. The area around the Exchange is the subject of 24-hour police presence under Operation Atlas, which includes visits by our heavily armed Hercules teams. We also established vehicle checkpoints at seven major intersections leading into the Exchange. Each is monitored by Stock Exchange security officers trained by the NYPD. Each checkpoint is outfitted with Police Department recommended equipment, including Delta barriers and sallyports to deter truck bombs; explosives screening points and bomb-resistant guard booths. Further protection is offered by dozens of retractable bollards and heavy planters that restrict pedestrian and vehicle blow.

I want to note that as lower Manhattan continues to recover, and continues its rebuilding process, we plan to dedicate significant resources and personnel to keep pace with the growth of business. That includes the establishment of a coordination center where all relevant law enforcement agencies and the private sector will be represented. We look forward to Federal support of such an initiative.

Mr. Chairman, any viable counter-terrorism program must stress prevention and response equally. And if, God forbid, New York City is struck again by terrorists or any other disaster, the Police Department will be prepared to respond immediately. We have trained approximately 12,000 of our officers in more advanced chemical, biological and radiological response to an attack involving weapons of mass destruction. We have also provided training to nearly all of our uniformed personnel in the New Citywide Incident Management System or SIMS, adopted last year by New York City. The system provides a unified command structure that allows the Police Department to work seamlessly with other first responders, including the Fire Department, for any disaster.

We conduct daily exercises throughout the city in responding to a terrorist attack. This constant training and drilling paid off during the blackout of 2003, when the Police Department was mobilized to protect the city from looting and potential disorder. There were few arrests and disruptions were kept to a minimum.

As you know, while overall evacuation planning is the responsibility of the city's Office of Emergency Management, the Police Department would play a major role in such an event. One of our most important responsibilities would be to secure key sites and protect life and property during and after a major incident. We're fully prepared to do that.

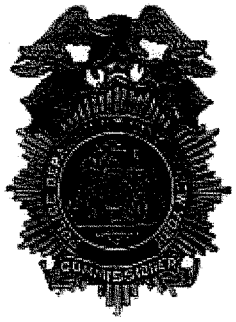
On that note, I want to mention that last week we welcomed back the second half of the 300-plus police officer contingent we sent to Mississippi and New Orleans after Hurricane Katrina. These officers took part in search and rescue operations and patrolled against looters. Along with the pride and satisfaction from a job well done, the Police Department will undoubtedly learn from that experience and we dispatched another joint New York City Police Department and Fire Department team to Texas to assist there with Hurricane Rita.

Finally, Mr. Chairman, I want to emphasize that all of our preparations come at a steep price; about 180 million per year to maintain our daily counter-terrorism and intelligence activity. These are ongoing operational costs to defend the city. While the Federal Government provides vital assistance for training, equipment and overtime, we still have huge expenses to cover. Regrettably, the influx of Federal support one would expect to flow to New York as a result of living in the cross hairs has not been sufficient.

The Police Department is defending New York's people, its infrastructure and the Nation's financial assets from another terrorist attack, yet a large proportion of the Federal homeland security grant funding still is not targeted to threat. The Federal Government must invest realistically in protecting those areas the terrorists are likely to target again. Along with a few other major cities, New York tops that list. Everything we know about al-Qaeda tells us that this is true. It's a lesson from our history that we simply cannot afford to ignore.

Thank you for inviting me today, Mr. Chairman.

[The prepared statement of Mr. Kelly follows:]



Raymond W. Kelly

Police Commissioner of the City of New York

Testimony Before
Subcommittee on Management, Finance and Accountability
of the Committee on Government Reform
U.S. House of Representatives

Homeland Security Preparedness in New York City

September 26, 2005
Brooklyn Law School, 250 Joralemon Street
Brooklyn, New York
10:00 AM

Chairman Platts, Congressman Towns, Members of the subcommittee. Good morning.

Defending the financial capital of the world from a terrorist attack is the number one priority of the New York City Police Department. Accordingly, I would like to focus my remarks today on the preventive measures the Department is taking against this threat.

As you know, one of the stated aims of Osama Bin Laden and Al Qaeda is to target America's economy. Shortly after the September 11th attacks, Bin Laden himself exulted in the massive blow suffered by the U.S. economy, offering in an interview his own estimation of over $1 trillion in losses. We have no doubt he seeks to replicate that strike.

Since then, we learned of another plan to target financial institutions in New York. This, after authorities discovered detailed surveillance of the Stock Exchange and the Citigroup Center in the laptop computer of an Al Qaeda operative captured in Pakistan last year.

This followed two additional Al Qaeda plots to target the city in 2003: the first to bring down the Brooklyn Bridge, and the second to smuggle weapons through a garment district business into the heart of Manhattan.

These plots were foiled by increased police visibility and good intelligence sharing. I cite them as evidence that New York City remains squarely in the crosshairs. Consequently, nowhere else is the effort to prevent another attack being undertaken with greater urgency.

In addition to the dollar cost, this has required that we divert a thousand police officers to counter terrorism duties every day, and engage in extensive training and preparation. We have also undertaken a range of defensive measures to protect and harden the downtown financial district, and enlist the support of the private sector.

Beginning in January 2002, we created a new Bureau of Counter Terrorism and we restructured our Intelligence Division. We recruited outstanding individuals with extensive federal intelligence and counter-terrorism experience to run them. We expanded our presence on the Joint Terrorist Task Force with the FBI. And we posted detectives to 7 other countries to enhance the flow of information we receive about any threats relevant to New York City.

We established one of the premier counter-terrorism training centers in the nation right here in Brooklyn. In addition to our own corps of 37,000 police officers, we have delivered training through that center to members of the New York City Fire Department; the Metropolitan Transportation Authority Police Department; the New York State Police; the Nassau, Suffolk, Westchester and Rockland County Police; and other agencies.

We have also brought in dozens of private security professionals from hotels, banks, and other institutions to train them in better ways to protect their facilities. Through our NEXUS program we are reaching out to businesses that terrorists might seek to exploit. We want businesses to report any unusual orders or anomalies that might suggest terrorist involvement. Detectives have paid thousands of visits to businesses throughout the city to increase their counter terrorism awareness.

In July, we launched a new initiative with the private security industry in New York called "NYPD Shield." We are establishing a secure website with training materials and threat updates, and we have offered detailed briefings on topics such as the London bombings and the attack on the Egyptian resort of Sharm el Sheikh. We also exchange threat information daily with the city's corporate and institutional security directors though an instant messaging system.

We have expanded the protection of critical infrastructure throughout the region. We have created the threat reduction and infrastructure protection program, or TRIPS. We have divided critical infrastructure into 5 categories, and assigned a team of detectives to cover each one.

These investigators visit facilities throughout the city, identifying vulnerabilities and developing comprehensive protection plans with site managers to prevent attacks.

In 2003, at the beginning of the war in Iraq, we implemented a comprehensive security plan known as "Operation Atlas." Given the ongoing terrorist threat, "Atlas" remains in effect today. Broadly speaking, Operation Atlas has tightened the protective net around the city by increasing vigilance at all entry points into New York, and by placing mass transit and other potential targets under much greater scrutiny.

Turning to the financial district itself:

Beginning in 2002, the Police Department engaged in extensive collaboration with the New York Stock Exchange and downtown business leaders to harden the financial district.

The area around the Exchange is the subject of a 24-hour police presence under Operation Atlas, which includes visits by our heavily-armed Hercules teams. We also established vehicle checkpoints at 7 major intersections leading into the Exchange. Each is monitored by Stock Exchange security officers trained by the NYPD. Each checkpoint is outfitted with Police Department-recommended equipment including Delta barriers and sallyports to deter truck bombs; explosives screening points; and bomb-resistant guard booths. Further protection is offered by dozens of retractable bollards and heavy planters that restrict pedestrian and vehicle flow.

I want to note that as lower Manhattan continues the recovery and rebuilding process, we plan to dedicate significant resources and personnel to keep pace with the growth of business. That includes the establishment of a coordination center where all relevant law

enforcement agencies and the private sector will be represented. We look forward to federal support of such an initiative.

Mr. Chairman, any viable counter-terrorism program must stress prevention and response equally. And if, God forbid, New York City is struck again by terrorists or any other disaster, the Police Department will be prepared to respond immediately.

We have trained approximately 12,000 of our officers in more advanced chemical, biological, and radiological response to an attack involving weapons of mass destruction. We have also provided training to nearly all of our uniformed personnel in the new Citywide Incident Management System, or CIMS, adopted last year by New York City. The system provides a unified command structure that allows the Police Department to work seamlessly with other first responders, including the Fire Department, for any disaster.
We conduct daily exercises throughout the city in responding to a terrorist attack. This constant training and drilling paid off during the blackout of 2003, when the Police Department was mobilized to protect the city from looting and potential disorder. There were few arrests and disruptions were kept to a minimum.

As you know, while overall evacuation planning is the responsibility of the City's Office of Emergency Management, the Police Department would play a major role in such an event. One of our most important responsibilities would be to secure key sites and protect life and property during and after a major incident. We are fully prepared to do that.

On that note, I want to mention that earlier this week, we welcomed back the second half of the 300-plus officer contingent we sent to Mississippi and New Orleans after Hurricane Katrina. Those officers took part in search and rescue operations and patrolled against looters. Along with the pride and satisfaction of a job well done, the Police Department will undoubtedly learn from that experience. And we have dispatched another joint New York City police and fire team to Texas to assist there with Hurricane Rita.

Finally, Mr. Chairman, I want to emphasize that all of our preparations come at a steep price: about $180 million per year to maintain our daily counter-terrorism and intelligence activities. These are ongoing operational costs to defend the city. While the federal government provides vital assistance for training, equipment, and overtime, we still have huge expenses to cover.

Regrettably, the influx of federal support one would expect to flow to New York as a result of living in the cross-hairs has not been sufficient. The Police Department is defending New York's people, infrastructure and the nation's financial assets from another terrorist attack yet a large proportion of the federal homeland security funding still is not targeted to threat.

The federal government must invest realistically in protecting those areas the terrorists are likely to try to hit again. Along with a few other major cities, New York tops that list. Everything we know about Al Qaeda tells us this is true. It is a lesson from our history we simply cannot afford to ignore.

Mr. PLATTS. Thank you, Mr. Kelly, we appreciate your testimony and glad to have an exchange with you. Just this past week we saw with Mayor Bloomberg announcing the $6 million grant from the Department of Justice regarding the interoperations of communications, through the city and the surrounding counties and boroughs of New York and New Jersey and that certainly goes to part of your message about coordination and the ability to be on the same page.

Can you expand a little bit on that effort and how that's building on the interoperable communications already in place since September 11th?

Mr. KELLY. We actually had interoperability capability before September 11th and since September 11th it's been reinforced and practiced indeed. We emphasize and check our interoperability channels every day. What this gives us is the ability to communicate with the surrounding areas; particularly Essex County in New Jersey and Bergen County and Westchester County. So in the event that our resources from those counties need to come into New York City or we respond to their purposes, we can communicate more effectively.

So it's certainly moving in the right direction. With support it will take perhaps about a year to get that function.

We do have now interoperability with Nassau County, which is contiguous to New York City, on our eastern border. So it's, again, part of the continuum to continuing to improve our ability to communicate.

Mr. PLATTS. The provision of the $6 million certainly is not perfect, and I know it's a challenge to acquire sufficient funds. You've touched in your testimony on the not-unlimited national funds, that we do it in a smarter way.

Are there specific examples of where the things that are currently you'd like to see done that stand before Department of Homeland Security or Justice to help fund some of the efforts here that are most critical to your efforts regarding a possible terrorist attack in general or specific to the financial sector?

Mr. KELLY. We incurred significant operational expenses to have our counter-terrorism program in place, that is, in essence, overtime expenses. I mention it in my prepared remarks, we spend about $180 million a year, Police Department, that is, to carry out our counter-terrorism functions. That's on top of other overtime expenses that we have in the normal course of protecting this city.

What we would like to see is in a general sense more money made available for those operational expenses. Much of the money that we have received is targeted for equipment and we certainly appreciate that and we need it, but we'd like to see if at all possible a broadening of the authority where we would get reimbursement that enables us to pay for operational expenses, particularly overtime expense.

Mr. PLATTS. Your testimony talked about 1,000 officers a day. That's year round you have 1,000 officers involved in training related to counter-terrorism?

Mr. KELLY. Yes, sir. Either officers or full time equivalent officers. We've created a counter-terrorism bureau, we expanded our intelligence division. We also have our preparedness program,

where we have responses, everyday drills where we take them off of normal patrol duties, have them come to locations—it can be throughout the city, but most of the locations, quite frankly, are in Manhattan, so we mobilize twice a day, we'll bring in as many as 100 radio cars, so two officers will come together twice a day to do that.

We then take them, mobilize, and then go to sensitive locations that we're concerned about. They don't go necessarily to the same location every day. We make certain we change the face of what we do, because we are concerned about reconnoissance going on. So that's part of our resource tactic, to make certain we constantly change what we do. But in doing that, and in training, as you say, it requires about 1,000 officers a day. So it's a significant commitment on the part of the city at a time when, right now as we speak, we are 4,500 officers below where we were in October 2000.

So not only have we reduced the head count because of budgetary reasons, we are supplying 1,000 officers for counter-terrorism forces. We're happy and it's a credit to the great job that the police officers of the city that crime is continuing to come down. As a result of their hard work, crime is down about 20 percent in the last 3½ years in New York City. It still takes a lot of hard work, a lot of effort, but we're juggling a few of balls in the air, as you can see.

Mr. PLATTS. I think across the country, I'm not a veteran myself of the military or a member of the law enforcement community and both communities have my great respect and admiration and our law enforcement here at home and the first responders are really the heroes of this war on terror, certainly in New York and the New York City Police Department.

In your coordination in trying to be prepared, whether it be communication or manpower, you talked about one, protecting infrastructure, and again, in the financial sector, or people in the—evacuation people if the financial sector was again targeted.

How is your coordination with National Guard? One of the challenges we saw in Katrina was how that coordination, Federal, State and local occurred. How often do you train with, interact with National Guard if they were trained to assist with either evacuation or control in New York City?

Mr. KELLY. There are actually National Guard troops in New York City now, certainly at Grand Central Station, Penn Station. When we have major events, we activate what we call an emergency operation center in Police Headquarters and we will have representatives from many city agencies, State agencies, Federal, including the National Guard, so they're physically located with us. I must also say private sector security also comes to our emergency operations center. So we're in the business of communicating and coordinating with them, at least the ones—for instance, last, well, it's now, the U.N. General Assembly is ongoing, but a week and a half ago we had the plenary session where we had more world leaders that have ever come to one spot in one building before, it was the 60th anniversary of the United Nations, so we activated that and within that center was National Guard, military, so we do it on a regular basis.

Mr. PLATTS. You mentioned the private sector in your NYPD Shield program, trying to have that communication. How can you

describe the buy-in or the involvement of the private sector communities with NYPD?

Mr. KELLY. They very much want to be working with us and certainly we want that as well, so there's a very collaborative, cooperative environment that exists in this city. We have had a program, the APL program, it stands for Area Police Liaison Program, it's been in existence since the 1980's, but we've strengthened that. We communicate with the people in that group virtually every day, by Blackberry, e-mail, letting them know what's going on on a daily basis. That program has been ongoing, as I say, and has been strengthened.

Now, NYPD Shield is sort of an umbrella program that incorporates that and other programs that we have. It is a proactive attempt on our part to do training, to bring them even closer to us, and it's been very well received. We have a Web site and we keep them informed of an ongoing situation. I said in my prepared remarks, we had a detailed briefing for them on the London bombings, we very much appreciate it. Just recently we had a briefing on the Sharm el Sheikh bombings in Egypt. We had an officer assigned to Israel, he was able to go there, came back with specific information. Showed him pictures, and as I said, we're communicating on e-mail all the time. So that organization has about 1,000 members.

But these are security directors. I mean, they're representative of the major corporations in New York City. These are the security people who really are protecting the financial services industry and other industries as well. So I'm very encouraged about Shield and I can only characterize our relationship with the private security and private sector as being a very strong and collaborative one.

Mr. PLATTS. I have some additional questions, but I want to yield. Before I do, I want to note that we're joined by Dean Wexler and I thank her for letting us be here today. As a law school graduate, I'm always hesitant to being in a moot court, I'm used to being out there and being judged, but I guess we're being judged differently today, but I appreciate your hosting us. Mr. Towns.

Mr. TOWNS. I'd like to echo the chairman's thanks, Dean, for allowing us to come in and also like to thank you, Commissioner, for coming.

In terms of funding for first response, from the Federal Government, can you describe for us the flaws or barriers that may be inherent with the current process? What are some of the problems that you see in the present process?

Mr. KELLY. As Mayor Bloomberg has stated many times and I've gone to Washington and testified that we would certainly support a funding allocation that would base totally on threat. To us it's logical. We see ourselves threatened and we would be the recipient of more funding, with some formula based on threat or at least more heavily based on threat than the existing formulas that were put in place.

Having said that, I mean, we need the money, but having said that, the Mayor has made certain that the department is getting everything that it needs, that we need, and he said that on many occasions. This strains the city's budget, though, no question about it. Money, we have to have a balanced budget every year, so the

money that's going to the Police Department, the Fire Department, other first responders is being taken from somewhere else in the city's budget. So we believe that a threat-based formula, a total threat-based formula makes sense in the post September 11th world that we live in.

Mr. TOWNS. You mentioned in your comments earlier about communications and of course information sharing. Have the industry stakeholders coordinated their certainly internal efforts with your department? Do you feel that industry has made adequate progress in developing comprehensive security practices that are appropriately based on risk and level of exposure? Do you feel comfortable?

Mr. KELLY. I think we can all do more. I think the private sector can do more, but I think efforts are being made, some industries, some companies do more than others. But, generally speaking, the message is out there, and as far as our relationship with them, you know, as I stated before, it's a very cooperative and close relationship. However, I think private, the private sector has gotten the message, but we could all do more.

Mr. TOWNS. Can you describe for us what lessons have been learned from New York PD and the city since 2001 as to the value of having industry and government as partners in information-sharing activities? Are there barriers to adequate information sharing that remain problematic for industry or Government participants? I'm concerned about this flow of information and communications.

Mr. KELLY. I believe it's better than it's ever been. As I said, our Shield, NYPD Shield program is all about information sharing. It's very well received by the private sector. We want to get information out, the Federal Government wants to get information out. There's a whole, there's an environment that supports information sharing now as never before in government, so nobody is holding on to information. Nobody wants to be caught holding on to information, quite frankly, so there's a lot of sharing going on.

As I said, we had, in the London bombings, it was all public information, but we really got in the weeds with our private security partners, giving them a lot more detailed information than most of them had. And it's our belief that the better informed they are, the better able they are to protect themselves and thereby protect the city. We can't do it alone, that's our message to them. We need your eyes and ears, we need your active support, your active involvement.

So I think prior to 2001, sure, I mean, we just didn't see the threat as we should have, but since 2001, it's gotten increasingly better as far as the sharing of information at all levels of government and government with the private sector.

Mr. TOWNS. I yield back, Mr. Chairman. Thank you.

Mr. PLATTS. Thank you, Mr. Towns. On the threat-based allocation, I was just reading your testimony in preparation for the hearing. It gave me as a member from South Central Pennsylvania a better idea of the challenges you face in allocation resources. In my District we have Gettysburg and some national sites of significance and certainly Philadelphia, but given how New York has been targeted not just in 2001, but in some of the intelligence since you ref-

erenced, back to 1995, the allocation, it certainly helps me to better understand the importance of that threat-based allocation approach.

When we were here for the convention last year and had a chance to visit the Police Museum, times have changed from some of what was shared in that museum to today. The fact that there are seven officers deployed in other countries, being out there, proactive in your intelligence efforts is quite a difference from 100 or so years ago.

One of the issues touched on about intelligence gathering and sharing intelligence, certainly within New York City and all your efforts, Federal, State and local, private sector. In Washington, one of the changes we made from September 11th was the Patriot Act, which was to allow information to be shared between those communities; intelligence gathering and law enforcement.

Are you able to share specific examples of how the changes we made at the Federal level helped you at the local level here in New York regarding intelligence gathering because of those statutory changes of the Patriot Act?

Mr. KELLY. Well, the Patriot Act helps the Federal Government, helps the FBI gather information, also exchange information or use information internally. It eliminated or greatly reduced the wall that existed in the FBI, for instance, between intelligence gathering and criminal investigation. So I know it's helped.

I can't give you specific examples where it applied to New York City, but I can only assume like in certain cases, for instance, well, the Peracca case which I mentioned in my prepared remarks, I can only hope that helped in the investigation itself. It eases the flow of information, to me that's a good thing, inside the Federal Government.

Mr. PLATTS. Thank you. The private sector and the various efforts that you have ongoing, reaching out to them, is there any financial contributions by the private sector to the city of New York or to the NYPD specific to acknowledge that there's a benefit to those private sector partners as well, maybe in a greater sense in some of your efforts, because it's really targeted, say, specifically to the financial sector, are there any resources that are allocated by them to your efforts?

Mr. KELLY. Of course, they would argue that their taxes are their contribution.

Mr. PLATTS. I would readily agree with them, but it's always good to ask if they want to give more.

Mr. KELLY. I can give you one example, though, that there was a contribution. That's with the protection of the New York Stock Exchange. I mentioned again in my prepared remarks how certain intersections are protected by individuals trained by the NYPD. Well, they're paid for by the New York Stock Exchange. They also pay for some paid detail police officers that we have assigned there, but we have active duty on-duty police officers working there as well. We have significant resources devoted down there, but they're paying for that heightened level of security there, and of course you could argue that as we bring together security folks throughout industry and the financial services industry and we sort of task them in an implicit way to do things for us, that they're contributing.

But that's the only hard example that I can give you of contributions where the New York Stock Exchange had paid significant amount of money for protecting the area around the Stock Exchange.

Mr. PLATTS. And I think a good example of that partnership, public and private.

I want to conclude in your testimony, you talked about continuing to adapt, especially with the business community here in the city with the coordination center between law enforcement and private sector and the need for Federal support for that initiative, and I assume that means funding support.

I want to give you the opportunity to expand with Treasury and Homeland Security who is here, and the two Members that are here, maybe a little bit about what that is and the importance of it.

Mr. KELLY. Yes, sir. The Freedom Tower is going forward at the 16-acre site of the World Trade Center. There will be other structures put in place there. Goldman Sachs has agreed to build onsite 26, which is right across from the Freedom Tower, so there's going to be a significant increase of people in the area and development, of course the financial services sector is going to be well represented.

As that development goes forward, we are committed, the city is committed to putting in additional resources in the area that will involve both personnel, but also technology, and we're studying that now and moving forward with it.

One of the plans that we have as that goes forward is to put in place, as I said, a coordination center, where we would have not only appropriate law enforcement agencies there, for instance, Metropolitan Transportation Authority, Port Authority, our own police personnel, Fire Department, but representatives from the stakeholders that will be there; the private sector security, and we envision that would be a 24-hour coordination center, and we've talked to industry leaders, they're enthusiastic about all this. But that's kind of our overall plan.

It's going to be expensive. We think it's important for us to provide additional protection in that area. Now, it will not only be limited to that area let's say, below Chambers Street. It will also be somewhat north. Some of the things we're doing now are under our Operation Atlas, as I said, we mobilize twice a day and send our units out to sensitive locations. We use some of these resources to do that, so it will be—it will help us in doing some of the coverage that now we're taking directly out of patrol resources and other parts of the city.

So that's kind of the overall plan. Yes, we certainly would like to have Federal resources to help whenever it could.

Mr. PLATTS. Thank you. Mr. Towns, do you have other questions?

Mr. TOWNS. Yes, I do. Thank you very much, Mr. Chairman.

The recent disaster in the Gulf Coast region demonstrates for us that major events do not have to be terrorist-related to have significant consequences. Have there been any significant efforts made by the New York City Department of Police or the city itself to establish evacuation plans for, say, Wall Street or lower Manhattan in the event of a major physical disaster? Have State and regional

stakeholders, such as Port Authority or MTA, been proactive in developing a comprehensive plan to move large volumes of people away from the disaster area in a safe and timely fashion? I guess the last part would be how can the Federal Government assist you in that process.

Mr. KELLY. We do have very comprehensive evacuation plans. Evacuation plans are coordinated by the Office of Emergency Management, but the Police Department plays a significant role in carrying out those plans. We provide assistance in evacuations, going to areas that may be evacuated. Search and rescue would be part of the functions we would provide. We have a coastal storm contingency plan and we have an evacuation plan for the entire city. The city is divided into 150 sectors, and there are elaborate plans for that. As a matter of fact, Commissioner Bruno, the head of the Office of Emergency Management is testifying right now at the City Council on those plans.

As far as the other stakeholders are concerned, yes, the Office of Emergency Management works with the Port Authority, MTA. Obviously MTA would provide a significant amount of the transportation used to evacuate areas of the city. We have, as you well know, Congressman, a very large public transportation system in the city; subway and buses. The MTA would be an integral part of any evacuation plan. Port Authority as well.

As far as Federal Government assistance, I can't think of anything specific. I'm sure Commissioner Bruno can think of it, but I can't think of anything that comes to mind for me other than any resources that could supplement what we're doing, anything that could help in the movement of people in a major evacuation, but we are, we have plans to evacuate every sector of the city, not just the financial district in lower Manhattan, but I must say that area is in one of the flood plans.

If you look at our coastal storm contingency plan, you'll see it's prefaced on certain assumptions; Category 1, 2, 3 and 4 storms. It does not go up to 5, but it does go up to 4, and there are flood areas in, say, lower Manhattan, that would be impacted by even a Category 1 storm. So there are plans to have an evacuation and also plans to provide services in that area, if something like a large storm hits us.

Mr. TOWNS. Let me say, Commissioner, we really appreciate your involvement in the kind of information that you shared with us in Washington, you know, but we need to sort of do a little bit more to make certain they fully understand. Because when I say to my colleagues in Washington that you have 1,000 police officers involved in counter-terrorism and they, knowing the Police Department is not even 2 percent the size of that, it's hard to communicate with them what this really means, the impact of it. Do you have any ideas or suggestions of what you might say to us or give to us that we may further take back to our colleagues to try to convince them that New York is unique in so many ways, and that this is the financial capital of the world and that New York is a place that we need to make certain that is protected in every way. So do you have anything that you might want to share with us further that we might be able to convey to our colleagues?

Mr. KELLY. I think every part of America, indeed, significant parts of the world would be adversely affected by another attack in New York. We know that al-Qaeda's goal is something bigger and better than September 11th. They're not looking at small bar events in this city, they're looking for something larger, and it's been stated in a lot of different ways. So anybody who thinks that it just affects New York City or New York State is mistaken.

We're protecting, as I said in my remarks, national assets. We're protecting assets that if they're attacked, will have an adverse impact across the world. You look at the things I mentioned. Look at New York Stock Exchange, you look at American Stock Exchange, NASDAQ. You look at the financial services industry headquarters that we have here. We have an attack here against any of those institutions, it will reverberate throughout the world, and certainly throughout America.

So I think that's the message that has to go back to Washington. We understand that people are concerned about their districts, that's what they're in Washington for. But you also have to look at the bigger picture. Because if we're struck here, it's going to hit in some way, shape and form, every congressional district in America and it's going to hit in a very hard way. The next event, God forbid, if there is one, is going to be, unfortunately, at least in their planning cycle, their planning minds, much larger than the last one.

Mr. TOWNS. Thank you. I yield back.

Mr. PLATTS. Thank you, Mr. Towns. Thank you, Commissioner for your insights. I appreciate certainly your current service here in New York, but I also mark your great service as a combat veteran in Vietnam and your 30 years in the reserves. As a fellow citizen, I'm personally grateful for your dedication to all of us citizens.

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

Mr. PLATTS. We'll take about a 2-minute recess here while we get our second panel: Mr. Parsons, Caverly and Muccia. Thank you.

[Recess.]

Mr. PLATTS. We'll reconvene here and again we're delighted to have our second panel here: Mr. Scott Parsons, Deputy Assistant Secretary, Critical Infrastructure Protection and Compliance Policy, Department of the Treasury. Glad to have you with us. Mr. James Caverly, Director of the Infrastructure Coordination Division, Department of Homeland Security and Mr. James Muccia, first deputy superintendent of banks.

Now that you're all seated, if I could ask you all to rise, we'll swear you in and proceed with your testimonies.

[Witnesses sworn.]

Mr. PLATTS. You may be seated. The clerk will note all three witnesses affirmed the oath. We'll proceed first with Mr. Parsons. If you'd like to begin, and again we'll use roughly a 5-minute guideline, but we're glad to hear your testimony in full.

STATEMENTS OF D. SCOTT PARSONS, DEPUTY ASSISTANT SECRETARY, CRITICAL INFRASTRUCTURE PROTECTION AND COMPLIANCE POLICY, DEPARTMENT OF THE TREASURY; R. JAMES CAVERLY, DIRECTOR, INFRASTRUCTURE COORDINATION DIVISION, DEPARTMENT OF HOMELAND SECURITY; AND DANIEL MUCCIA, FIRST DEPUTY SUPERINTENDENT OF BANKS, STATE OF NEW YORK BANKING DEPARTMENT

STATEMENT OF D. SCOTT PARSONS

Mr. PARSONS. Thank you very much. Chairman Platts, Ranking Member Towns, thank you very much. We really appreciate the opportunity to be here today to testify on the financial services sector preparedness to handle a wide scale disruption.

Mr. PLATTS. Mr. Parsons, do you mind holding that a little closer? I can hear you, but I'm not sure if everyone can. Thank you.

Mr. PARSONS. I am pleased to tell you that the financial sector has made tremendous progress to insure its resiliency to withstand both man-made and natural disasters. President Bush has led the development and implementation of an effective program to defend our country's critical infrastructure. The financial services sector plays an indispensable role in the Nation's economic system, providing individuals, businesses and the government with credit and liquidity, short and long term investments, risk transfer products, various payment systems and depository services. It enables people to save for their education, their retirement, to purchase their homes and to invest in their dreams.

The financial services system is essential to America's overall economic well-being. I note that we have experienced a number of events in recent years that test the resilience of the sector. The attacks of September 11, 2001, the power outage of August 15–16, 2003 and the elevated threat level for the financial sector of August 2004 have all tested the preparedness and resolve of the financial services sector. Most recently, Hurricane Katrina caused unprecedented devastation in multiple States. Yet the financial system has survived each of these events and through hard work and investment becomes stronger and better able to withstand such disruptions.

The President has mandated that the Federal Government work closely with the private sector to protect the Nation's critical assets and infrastructure from major disruption. An important and unique insight that guides this strategy is that nearly all of the financial infrastructure is owned by the private sector, and, therefore, the success of our protective efforts depends on close cooperation between the Government and the private sector. On December 17, 2003, the President issued Homeland Security Presidential Directive No. 7 which establishes a national policy for Federal departments and agencies to identify and prioritize U.S. infrastructure and key resources and protect them from terrorist attacks. HSPD7, as it's known, recognized that various departments and agencies have specific knowledge, expertise and experience in working with certain sectors. Therefore, this directive provided for sector specific agencies or lead agencies for given sectors and the Department of Treasury has been designated as a sector specific agency for the banking and finance sector.

It is under this designation that Treasury collaborates with appropriate private sector entities and other governmental agencies to encourage the development of information sharing and analysis mechanisms and to support sector coordinating mechanisms with the purpose of, No. 1, identifying, prioritizing and coordinating the protection of critical infrastructure, and, No. 2, to facilitate the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures and best practices.

Secretary Snow has a very strong commitment to insuring that the financial system continues to serve all Americans. The Nation's economy has been a constant target of terrorists who wish to do us harm. A consistent part of the rhetoric from Osama bin Ladin and others is the overall ideology to attack our Nation's economy, to attack the financial system to support it and to try to do us harm in this manner.

Secretary Snow has tasked the Treasury Department's Office of Critical Infrastructure Protection and Compliance Policy to be responsible for developing and executing policies affecting both the physical and the cyber security of the U.S. financial system. The majority of these efforts require close cooperation and partnership with the public and private sector, and there are a number of important groups that we work with to achieve this end. One is the Financial and Banking Information Infrastructure Committee. This is a body of all of the Federal and State financial regulators and the Treasury Department is the Chair of this committee.

The second is a private sector body, the Financial Services Sector Coordinating Council. You'll be hearing from the Chair of the FSSCC, as it's known, later on this morning.

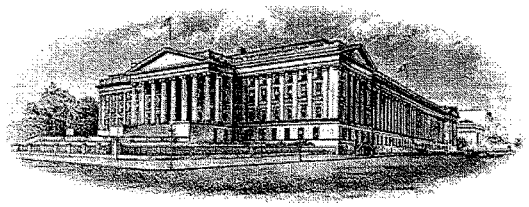
We also utilize an important information sharing mechanism called the Financial Services Information Sharing and Analysis Center or the FS–ISAC. That is a body that is run by the private sector with the sole purpose of disseminating critical physical and cyber threat information to the financial services sector members.

And last, I would mention an important development, something that we think holds great promise and that is the creation of regional coalitions. I note specifically, Ranking Member Towns mentioned the futures industry. The first coalition of this nature is called ChicagoFIRST. It was based in Chicago with the recognition that the futures industry plays a prominent role in that city, and its goal by its members was to advance homeland security protective measures, specifically with local emphasis on it.

We believe that this was a great model and we were able to partner with several other entities, including BITS, to document the steps that went into creating this and we've since published that document. I'm pleased to tell you that there is considerable focus on this initiative within the Department of Treasury and we are close to seeing some new announcements for new regional coalitions that will involve not only those on the east coast, but hopefully the west coast as well.

With that, Mr. Chairman, I conclude my opening comments.

[The prepared statement of Mr. Parsons follows:]



DEPARTMENT OF THE TREASURY
OFFICE OF PUBLIC AFFAIRS

Embargoed Until 10 a.m. EDT
September 26, 2005

CONTACT: Brookly McLaughlin
(202) 622-1996

Statement by D. Scott Parsons, Treasury Deputy Assistant Secretary for Critical Infrastructure Protection and Compliance Policy, before the U.S. House of Representatives, Committee on Government Reform, Subcommittee on Government Management, Finance, and Accountability

Financial Market Preparedness for Wide-Scale Disasters or Disruptions: A Treasury Perspective

Introduction

Chairman Platts, Vice-Chair Foxx, Ranking Member Towns, thank you for inviting me here today to testify on the financial services sector's preparedness to handle a wide scale disruption. I am pleased to tell you that the financial sector has made tremendous progress to ensure its resiliency to withstand both manmade and natural disasters. President Bush has led the development and implementation of an effective program to defend our country's critical infrastructure. The financial services sector plays an indispensable role in the nation's economic system, providing individuals, businesses, and the government with credit and liquidity, short and long-term investments, risk-transfer products, various payment systems, and depository services. It enables people to save for their education, retirement, to purchase their homes, and to invest in their dreams. The financial services system is essential to America's overall economic well being.

I note that we have experienced a number of events in recent years that test the resilience of the sector. The attacks of September 11, 2001, the power outage of August 14 – 15, 2003, and the elevation of the threat level for the financial sector in August 2004 have all tested the preparedness and resolve of the sector. Most recently, Hurricane Katrina caused unprecedented devastation in multiple states. Yet the financial system has survived each of these events, and through hard work and investment, becomes stronger and better able to contend with such disruptions.

Organizing to Protect the Critical Financial Infrastructure

President Bush has mandated that the Federal Government work closely with the private sector to protect the nation's critical assets and infrastructure from major disruption. A unique insight that guides the Administration's strategy is that nearly all of the financial infrastructure is owned by the private sector. Therefore, the success of our protective efforts depends on close cooperation between the government and the private sector.

On December 17, 2003, our President issued Homeland Security Directive 7 (HSPD-7), which establishes a national policy for Federal departments and agencies to identify and prioritize United States infrastructure and key resources and to protect them from terrorist attacks. HSPD-7 recognized that various Departments and agencies have specific knowledge, expertise, and experience in working with certain sectors. Therefore, this directive provided for Sector Specific Agencies, or lead agencies, for given sectors. The Department of the Treasury is designated as the Sector Specific Agency for the banking and finance sector.

Under this designation, the Treasury collaborates with appropriate private sector entities to encourage the development of information sharing and analysis mechanisms, and to support sector-coordinating mechanisms to: (1) identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and (2) facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.

As the lead agency for the financial services sector, the Treasury fulfills its responsibilities under HSPD-7 primarily through the encouragement and support for the development and use of public-private partnerships. I will discuss these partnerships and other related efforts that serve to coordinate relevant parties and provide for the sharing of information.

Secretary Snow has a strong commitment to ensuring the financial system continues to serve all Americans. He has tasked the Treasury Department's Office of Critical Infrastructure Protection and Compliance Policy to be responsible for developing and executing policies affecting the physical and cyber security of the United States financial system. The majority of these efforts require close cooperation and partnership with the public and private sector. In carrying out these efforts, the Treasury continues to:

- Work with government agencies, private sector firms, national and regional organizations to have each establish a single points of contact for critical financial infrastructure issues;
- Promote strong relationships between financial institutions and the State and local governments where their operations are located;
- Inform the private and public sectors about the available resources that protect the financial infrastructure; and
- Support the availability of accurate and timely information about potential threats on a national and regional level.

National Partnerships

Following the attacks of September 11, 2001, the Department reacted quickly to organize the financial services sector. First, it initiated an intensive evaluation of the threats against the sector, and then analyzed efforts to address any potential vulnerabilities. To more effectively focus efforts and resources on these goals, the Treasury Department established a single point of contact within relevant public and private entities – the Financial Services Sector Coordinating Council for the private sector and the Financial and Banking Information Infrastructure Committee for the public sector group. I understand that you will be receiving testimony later from the head of that private sector council.

Financial and Banking Information Infrastructure Committee

To coordinate Federal efforts and to ensure the sharing of vital information, and pursuant to an Order by the President[1], the Treasury Department chairs the Financial and Banking Information Infrastructure Committee (FBIIC), and held its initial meeting on January 10, 2002. The President's Working Group on Financial Markets sponsors the FBIIC and oversees its role of coordinating the efforts of Federal financial regulators on critical financial infrastructure issues. The FBIIC, composed of Federal and State financial regulators, coordinates efforts to ensure the resilience of the financial system in the face of major disruptions. The Treasury Assistant Secretary for Financial Institutions chairs the FBIIC, which includes experienced representatives from almost 20 organizations that have regulatory authority over different segments of the financial services sector.[2] I have had the privilege and responsibility to serve as Acting Chair since January 2005.

The FBIIC has made significant achievements through the collaboration of its members. These accomplishments include: analyzing the critical infrastructure assets; the analysis of the financial services sector's dependencies on the energy, transportation, telecommunications, and information technology sectors; and the sharing of critical information among Federal, State, and local authorities.

Furthermore, the FBIIC has published reports with the Financial Services Sector Coordinating Council. These publications include "Lessons Learned by Consumers, Financial Sector Firms, and Government Agencies during the Recent Rise of Phishing Attacks" and "Impact of the Recent Power Blackout and Hurricane Isabel on the Financial Services Sector."[3] For each publication, individuals from the FBIIC and Financial Services Sector Coordinating Council solicited and collected written contributions from their member organizations.

The FBIIC agencies have done much for the recovery from Hurricane Katrina, and I have been privileged to work with so many selfless individuals in the Federal, State, local, and private sectors. During the events surrounding Katrina, the FBIIC met frequently, often several times a day, in order to share and exchange information to help the recovery effort by the financial sector. Although much work remains, I'm pleased to report that every financial institution in the impacted areas is now in an operating capacity.

Financial Services Sector Coordinating Council

The Department encouraged the creation of a corresponding entity to the FBIIC within the private sector. This organization, the Financial Services Sector Coordinating Council (FSSCC), develops and coordinates major policy issues for the private sector regarding the protection of the critical financial infrastructure. The FSSCC was inaugurated on June 19, 2002 in the Cash Room of the Treasury Building.

The FSSCC fosters and facilitates the coordination of financial services sector-wide voluntary initiatives to improve critical infrastructure protection and homeland security. The Department designates the chair of the FSSCC, whose membership consists of financial trade associations and organizations.[4] The FSSCC member trade associations represent the majority of the financial services sector.

---

[1] E.O. 13231, October 16, 2001

[2] Commodities Futures Trading Commission (CFTC), Conference of State Bank Supervisors (CSBS), Farm Credit Administration (FCA), Federal Deposit Insurance Corporation (FDIC), Federal Housing Finance Board (FHFB), Federal Reserve Bank of New York (FRB NY), Federal Reserve Board (FRB), , National Association of Insurance Commissioners (NAIC), National Association of State Credit Union Supervisors (NASCUS), National Credit Union Administration (NCUA), North American Securities Administrators Association (NASAA), Office of the Comptroller of the Currency (OCC), Office of Federal Housing Enterprise Oversight (OFHEO), Office of Thrift Supervision (OTS), Securities and Exchange Commission (SEC), and Securities Investor Protection Corporation (SIPC).

[3] These publications are available at http://www.treas.gov/offices/domestic-finance/financial-institution/cip/.

[4] America's Community Bankers, American Bankers Association, American Council of Life Insurers, American Insurance Association, American Society for Industrial Security (ASIS) International, Bank Administration Institute, Bond Market

The FSSCC is vitally important to our efforts to coordinate across the financial sector. We are fortunate that we have Don Donahue as the financial sector coordinator and chair of the FSSCC.

The members of the FBIIC and FSSCC meet together several times a year to share information and discuss progress on various initiatives and emerging concerns. These meetings give representatives from the public and private sector an opportunity to inform each other of their respective projects and successes. For example, during the March 2005 meeting, members of the FBIIC and FSSCC discussed the Department of Homeland Security's National Infrastructure Protection Plan, as well as the FBIIC and FSSCC plans for 2005.

Regional Partnerships

One of the insights on preparedness that we recognize is that any disruption will first and foremost require a rapid local or regional response. After establishing the national partnerships, the Treasury Department turned its attention to the support of regional partnerships. Because the financial community in New York City already had ties to the New York City Office of Emergency Management the Treasury Department turned its attention to Chicago, Illinois. Chicago's financial services industry is among the most diverse in the United States, and encompasses futures and securities exchanges, large and small banks, futures and securities clearinghouses, and check clearing and cash operations. Beginning in the summer of 2002, the Treasury Department met with and assisted financial institutions in Chicago that had an interest in coordinating homeland security efforts for downtown businesses.

In early 2003, several Chicago financial firms came together to discuss joining forces to address their common business continuity concerns. Their efforts produced a new kind of organization, named ChicagoFIRST, devoted to building and maintaining relationships between the financial community and the city, State, and Federal government, especially with law enforcement and emergency response officials. ChicagoFIRST's unique membership consists of financial institutions with a variety of charters and licenses, including national banks, insurance companies, securities and futures firms, securities and futures exchanges, and clearing organizations[5]. ChicagoFIRST fosters relationships with the public sector, trade associations, and other entities through periodic meetings with its "Strategic Partners."[6]

The Department of the Treasury has worked closely with ChicagoFIRST to improve its effectiveness as a regional coalition. In March 2003, the Treasury Department asked the City of Chicago to provide ChicagoFIRST a seat at the City's Joint Operations Center, which the City provided a few months later.

Association, ChicagoFIRST, Chicago Mercantile Exchange, Clearing House , Consumer Bankers Association, Credit Union National Association, Depository Trust & Clearing Corporation (DTCC), Fannie Mae, Financial Services Information Sharing and Analysis Center (FS-ISAC), The Financial Services Roundtable/BITS, Futures Industry Association, Independent Community Bankers of America, Investment Company Institute, Managed Funds Association, NASDAQ Stocl Market., National Association of Federal Credit Unions, National Association of Securities Dealers (NASD), NACHA — The Electronic Payments Association, Options Clearing Corporation, Securities Industry Association (SIA), Securities Industry Automation Corporation (SIAC), and VISA USA Inc.

[5] ABN/AMRO/LaSalle Bank; Allstate; Archipelago; Bank of America; Bank One; Chicago Board of Trade; Chicago Board Options Exchange; Chicago Federal Home Loan Bank; Chicago Mercantile Exchange; Chicago Stock Exchange; Harris Bank; Mesirow Financial; Mizuho Securities USA Inc; Northern Trust Bank; The Options Clearing Corporation; UBS; and William Blair & Company.

[6] ChicagoFIRST's Strategic Partners include the City of Chicago, the U.S. Department of the Treasury, the Department of Homeland Security, BITS – the Financial Services Roundtable, the Securities and Exchange Commission, the Commodity Futures Trading Commission, the Federal Deposit Insurance Corporation, the Illinois Commissioner of Banks and Real Estate, the Federal Reserve Bank of Chicago, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, U.S. Secret Service, the Federal Bureau of Investigation, the Financial Services Sector Coordinating Council, and the Futures Industry Association.

In August 2003, the Treasury Department, the FSSCC, and ChicagoFIRST members participated in a seminar for the City of Chicago on the criticality of the Chicago financial community. In July 2004, the Treasury Department sponsored in part an emergency response exercise for Chicago's financial community and Federal, State, and local government officials. This exercise tested the assumptions and emergency response plans of Chicago's financial community, the City of Chicago, the State of Illinois and the Federal Government. In December 2004, the Treasury Department, in conjunction with BITS and other parties, published a report on the ChicagoFIRST as a model for regional coalitions, entitled *Improving Business Continuity in the Financial Services Sector: A Model for Starting Regional Coalitions.*[7]

There have been preliminary discussions on forming new coalitions in Miami/South Florida, the San Francisco Bay Area, and Tampa Bay. We will continue to work encourage other cities and regions to embrace this important concept. We believe that regional coalitions such as ChicagoFIRST are essential to protecting and strengthening the financial services sector.

Outreach

With the primary support of the Federal Deposit Insurance Corporation, the FBIIC and the FSSCC have held a series of conferences in cities across the country, entitled "Protecting the Financial Sector: A Public and Private Partnership." The first conference was held in May 2003 in Chicago. In January 2005, the 29th and last conference in this series took place in New York City. These conferences, which reached over 4,000 individuals in the financial services industry, highlighted the importance of public-private cooperation to minimize the effect of manmade and natural events on the financial sector.

The conferences brought together public officials and experts from the private sectors who, in various ways, protect the nation's critical financial infrastructure. These individuals included United States Secret Service Special Agents, officials from the Departments of the Treasury and Homeland Security, representatives of the FBIIC and FSSCC, and members of ChicagoFIRST. The speakers at the conferences stressed the importance of joining or forming a public-private partnership to ensure the continued operation of the region's financial services sector in the face of adverse circumstances. This type of training, I believe, assists and has positively helped financial services professionals in recovering from incidents like Katrina.

Financial Services Information Sharing and Analysis Center

In 1999, with the encouragement of the Department, several leading financial institutions formed the Financial Services Information Sharing and Analysis Center (FS-ISAC) to share information about physical and cyber threats to the financial services sector. The FS-ISAC analysts gather information from financial services providers, commercial firms, Federal, State and local government agencies, law enforcement and other resources for secure dissemination.

The Department of the Treasury has long supported the FS-ISAC in its efforts to disseminate important information to the entire financial services sector. In addition to advising the FS-ISAC board, Department officials have worked closely with the organization and publicly supported its efforts. For example, in September 2004, the Secretary of the Treasury held a meeting with FS-ISAC members to commend their commitment to financial services sector resilience and their involvement in the public-private partnership.

In 2003, the Department commissioned an independent study of the FS-ISAC to determine its value to the financial services sector. The study found that members of the FS-ISAC benefited from its services, but that the former structure of the FS-ISAC only served a small portion of the financial services sector.

---

[7] This report is available at http://www.treas.gov/offices/domestic-finance/financial-institution/cip/.

In response to this conclusion, the Department then acquired $2 million in services from the FS-ISAC, with the effect of thereby making the Next Generation FS-ISAC a reality. By December 2004, all five Next Generation projects were completed: 1) a metrics dashboard to display key statistics related to value, membership, and alert volume; 2) alert dissemination confirmation; 3) a cyber security baseline; 4) secure online chat; and 5) the ability to process commercial security feeds. The Next Generation project has improved the FS-ISAC's ability to share threat warnings with the financial services sector.

National Communication Systems Programs

The Department of Homeland Security's National Communications System (NCS) administers a number of telecommunication programs in which the private sector participates. These programs include the Government Emergency Telecommunications Service (GETS), the Wireless Priority Service (WPS), and the Telecommunications Service Priority (TSP). The GETS program allows participants to receive priority access to the public telephone network if there is heavy traffic on the system. The WPS grants priority service to those calling from a cellular telephone. The TSP program grants participants priority restoration for very important telecommunications lines.

Through the sponsorship of the Department, critically important financial services sector institutions are eligible to participate in this program. The FBIIC Federal financial regulators consider the applications of the financial institutions and determine which are eligible for the programs. These programs have been successfully promoted through numerous FBIIC and FSSCC initiatives.

From Preparation to Action

The Department takes its responsibility to ensure and enhance the resilience of the financial services sector very seriously and realizes that it can only be done through cooperation between the government and the private sector. Since September 11, 2001, the Department has pursued an aggressive agenda working with the public and private sectors to prevent or diminish major disruptions to the financial sector in the event of a natural or manmade disaster. The Department has worked with key institutions, in participation with State and local officials, to ensure their business continuity plans are sound and effective.

Conclusion

We need look only to devastation caused by Hurricane Katrina to remind us of the need to prepare for large scale disasters. Our efforts to minimize the impact of crises, as they may occur in the future, are grounded in the President's goals and vision for the Treasury Department – a vision that is based on a shared commitment by the Federal government, the financial services sector, and State and local government, to prevent incidents from occurring where possible, and a vision that emphasizes preparation for events, so as to minimize their extent, and speed recovery. I am constantly reminded of what President Lincoln told us all more than 140 years ago: "Leave nothing for tomorrow which can be done today." Those words continue to guide us all as we face incidents that challenge our age, and the 21st century.

Thank you.

-30-

Mr. PLATTS. Thank you, Mr. Parsons. Mr. Caverly.

STATEMENT OF R. JAMES CAVERLY

Mr. CAVERLY. Mr. Chairman, Mr. Towns thank you for having us here today. What I'd like to do is summarize my comments and enter my statement into the record.

As we're all aware, protecting the Nation's critical infrastructure is really a partnership and it's a new kind of partnership between the owners and operators of that sector. Most of them being in the private sector and then State government, local government and Federal Government. Your panel of witnesses today I think does a great job of exemplifying exactly what kind of partnership needs to be there to insure that the Nation's critical infrastructure is protected the way we need to protect it.

Clearly, the events of September 11th, the power outage of 2003, then the casing reports heightened financial alerts in 2004 identifies the impacts that terrorism or threats of terrorism can have to the financial communities of this country and as Police Commissioner Kelly said, those impacts will reverberate across the country.

The Department of Homeland Security really has three principal objectives when dealing with critical infrastructure. One is to provide the resources and training to State and local government and law enforcement training for security enhancements. The other is to provide information to those various levels, whether they're the owners and operators of the individual components of the Nation's infrastructure, to local level law enforcement, State law enforcement and then across the Federal partnership of the kind of information that is necessary for each of those people to create risk assessments and react appropriately within the environment in which they're responsible for. And then underneath that is the creation of a fluid and viable information-sharing mechanism that will allow us to get the information quickly out to the points of decision and bring back information into the analytical framework that allows to us look at this as a total picture.

As Mr. Parsons identified, the President's directive to his cabinet contained in HSPD7, Homeland Security President's Directive 7, a key component of that is asking members of the private sector to create a framework in which we can deal with the sector as an entity. The financial services sector was the first sector to come across and create a single entity called the Sector Coordinating Council, and you'll be hearing from Mr. Donahue the head of the FSSCC later. Looking at that and looking at what was done in Treasury with some activities of our own, we implemented the National Infrastructure Protection Plan a framework across all of the sectors to create a set of sector coordinating councils and government coordinating counsels that will allow us to act on this partnership. We believe the financial services has shown us a great way in which to build this framework.

The other thing that HSPD7 directs the department to do is develop a National Infrastructure Protection Plan that is looking at setting security goals, identifying assets and assessing new risks. The NIPP plan was put out in a base plan in February of this past year. The next version will be coming out shortly. Once we get the base plan out in the next short timeframe, we'll begin working with

each of the critical infrastructure sectors to develop a sector specific plan that focuses on each of the sectors and the activities the various players have to do both at Federal, State, local and also private sector level.

A key component of one of the things that the department is working on is a risk assessment methodology. Secretary Chertoff has made risk assessment a key component of his program to enhance the Nation's critical security infrastructure. We developed a Risk Assessment Methodology for Critical Asset Protection [RAMCAP]. As we implement and develop the data inside, it will allow us to assess the risk across the infrastructures and do it comparatively. Because of the connected nature of the infrastructure, this is very, very important.

As I said earlier today, the panel here reflects a good level of the coordination and integration that needs to take place. We believe that the activities of August 2004, which led us to heighten the Homeland Security alert level in New York and Washington in the financial services sector is a very good example. As the intelligence was developed, we began working very closely with NYPD and the owners and operators and security directors in specific facilities that have been surveilled. We were able to take very quick and appropriate action across not only the responsibility of what local law enforcement and Chief Kelly were able to do, but also the owners and operators were able to do and share information. We think that is an example of exactly how this partnership should work because each of us has certain responsibilities in the framework.

One of the things about the financial services sector is the redundancy that is built into the system. Because of things that happened in the financial services sector in the 1980's and 1990's, when in fact it lost power in lower Manhattan and when it lost telecommunications at certain times, it built resiliency into its system. It has a very, very robust, resilient system to allow it, as the chairman pointed out, to resume its financial operations quite soon after taking a serious blow. We think that's important.

The national communication system is part of Department Homeland Security and we're working closely with the financial services sector to insure the telecommunication backbone for their information flows has the kind of resiliency and redundancy necessary to insure that no matter what happens the transactional part of that connectivity can continue.

One of the most important parts is a program we call "route diversity methodology." It insures as you look at the networks of the telecommunications that in fact all transactions are moving across a very diverse network, as opposed to being funneled into single hubs and therefore building a resiliency outside of that.

The last thing I'd like to make a brief comment about is Homeland Security Information Network. It is a framework the Department of Homeland Security is deploying that will allow us to connect to the various groups, whether regional groups or things such as the Financial Services ISAC. It is a cohesive network that allows a sharing of information not only inside the sector, but across sector lines and also across jurisdictional lines to insure that the information part that flows either to or from the Department of Homeland Security is accessible, whether it's law enforcement in-

formation, first responder information or information that we receive from the private sector.

With that, Mr. Chairman, I'll take your questions.

[The prepared statement of Mr. Caverly follows:]

Statement of R. James Caverly, Director, Infrastructure Coordination Division
US Department of Homeland Security
New York Field Hearing
September 26, 2005

Introduction

Good morning, Mr. Chairman and distinguished Members of this Committee. I appreciate this opportunity to speak with you regarding the current state of preparedness within the financial services sector, one year following the heightened threat level for the financial services sector.

We know al-Qaida targeted the U.S. financial sector critical infrastructure in the past and that this remains a potential target for the future. September 11th impacted the financial sector especially hard, with the simultaneous loss of critical financial infrastructure operational capacity and a precipitous loss of financial asset values. However, the financial sector remained resilient, and critical financial operations, including securities, trading resumed after only a few days of interruption.

Since September 11th other events, including the northeast power outage of August 2003, and the revelation of the financial casing reports in August 2004, continue to remind us that ensuring the financial sector is prepared for large-scale natural or man-made disruptions is essential

National Infrastructure Protection Plan

The Department of Homeland Security is committed to working with our partners in State, local and tribal governments and the private sector to reduce the overall level of risk of terrorist attacks against our national critical infrastructure. We help the national critical sectors to reduce risk by examining the consequences of a potential attack; examining the vulnerability of critical sites and facilities to various modes of attack; and examining the potential threat — that is, the intent of terrorists to attack in a given place and their likelihood of success.

In working to reduce risk and protect critical infrastructure, DHS has three principal objectives:

- Provide resources and training to State and local governments and law enforcement for security enhancements
- Provide information to both public and private sectors on the threat environment, tactics and techniques of terrorists, common vulnerabilities and suggested protective measures
- Create information-sharing mechanisms that enable DHS stakeholders to share amongst themselves information and best practices detailing the unique aspects of their assets to better ensure that DHS has adequate situational awareness during a crisis or when faced with a specific threat.

These goals are being realized through the implementation of the National Infrastructure Protection Plan (NIPP). Directed by Homeland Security Presidential Directive 7 (HSPD-7), the NIPP is a unified national plan for the consolidation of critical infrastructure protection activities. The NIPP is a collaborative effort between the private sector, State, local, territorial and tribal entities and all relevant departments and agencies of the Federal government.

The cornerstone of the NIPP is a risk management framework that combines threat, vulnerability, and consequence information to produce a comprehensive, systematic, and informed assessment of national or sector risk that drives our risk reduction efforts in the critical infrastructure/key resources (CI/KR) sectors. This framework applies to the general threat environment as well as specific threats or incident situations.

NIPP Risk Management Framework

The National Infrastructure Protection Plan incorporates the following objectives:

Set Security Goals. Achieving a secure, protected, and resilient infrastructure requires a common set of national and sector-specific security goals that address those aspects of risk that can be affected and collectively represent an acceptable security posture. Nationally, the overall security goal of risk reduction efforts is an enhanced state of CI/KR security achieved through implementation of focused risk reduction and protective strategies across the critical sectors.

Identify Assets. Once security goals are set, the next step in the framework is to develop and maintain an inventory of the Nation's critical assets. To identify these assets, DHS uses a screening process that helps us to identify those assets that present the greatest risk. However, before screening the assets, asset information is collected and catalogued in the National Asset Database, which is the central Federal repository for national infrastructure-related information. After an asset is identified and basic information on it is collected, DHS employs an initial screening methodology to determine whether or not it is of national consequence.

Assess Risk. If an asset is determined to of national consequence, it is then subjected to a risk analysis. As mentioned before, risk is determined by combining assessments of:

- Consequence — estimates of the damage that a successful attack would cause
- Threat — estimates of the likelihood that a particular target or type of target will be selected for attack.
- Vulnerability analysis determines which elements of infrastructure are most susceptible to attack and how attacks against these elements would be most likely be carried out.

One of the Department's principal risk-assessment tools is RAMCAP (Risk Assessment Methodology for Critical Asset Protection). RAMCAP is currently being developed by DHS in collaboration with other federal agencies and the private sector as a sector-

specific consequence, vulnerability, and risk methodology. RAMCAP will allow DHS to assess national critical infrastructures according to these factors and allows us to compare assets from across sectors and better prioritize our protective efforts.

Prioritize. It is impossible to protect all CI/KR equally across the entire United States. Because the potential consequences of an attack, threats, and vulnerabilities differ for individual assets and sectors, analysis is necessary to understand and prioritize risk across the infrastructure or various segments. Such analysis identifies high-risk assets that become the focus of longer-term resource decisions, strategic protective programs, and planning for response and other contingency situations. This, in turn, supports the informed allocation of resources and is the primary goal of the risk management framework.

Implement Protective Programs. The highly distributed nature of infrastructure demands distributed ownership and execution of protection programs, but it also requires centralized leadership to drive consistent implementation and ensure the greatest cost-benefit. DHS leads the Federal critical infrastructure protection effort, and works in collaboration with State and local government, the private sector, and our international partners to reduce our vulnerability to, among other things, bombing attacks, and to enhance our capability to respond if such an attack takes place.

Financial Sector Coordinating Councils

Private sector-led Sector Coordinating Councils (SCCs) and their counterpart, Government Coordinating Councils (GCCs), provide an important mechanism for effective public-private partnerships, information sharing, and coordination for the entire range of critical infrastructure protection, recovery, and response activities, both within and across sectors. Under the NIPP framework, DHS is encouraging the creation of SCCs for each of the 17 critical infrastructure/key resource (CI/KR) sectors. These councils are self-organized and self-governed and composed of sector owners and operators and their representative organizations. GCCs have been formed to achieve inter-agency coordination and information sharing on critical infrastructure protection activities. Like the SCCs, the GCCs coordinate strategies, activities, policy, and communication across organizations within each sector. The SCCs and GCCs serve as points of entry, coordination, and collaboration between government and industry in the sector.

The financial service sector has well-established coordinating council structures already in place. The sector is coordinated by the Financial Services Sector Coordinating Council (FSSCC), representing private sector companies, and the Financial and Banking Infrastructure Information Council (FBIIC), representing government regulators. The mission of the two groups is to improve the reliability and security of financial information infrastructure and to improve critical infrastructure protection and homeland security.

The FSSCC, a network of financial trade associations and private firms representing thousands of financial services organizations, works closely with the U.S. Department of

the Treasury, financial regulators, and the FBIIC to coordinate the private sector's work to identify and reduce vulnerabilities in the financial services sector infrastructure to organized attacks, criminal or illegal activities, or other disruptive events that may occur, to ensure the resilience of the nation's financial services sector infrastructure, and to promote public trust and confidence in the financial services sector's ability to withstand and recover from events that may occur.

Financial Sector Heightened Alert Level

The financial sector's vigilance in strengthening its resilience and crisis response procedures was clearly illustrated in its rapid response to last year's August elevation of the Homeland Security Threat Advisory level for the financial services sector in New York, northern New Jersey, and Washington, DC.

On August 1, 2004, the day the threat level was elevated, DHS held numerous urgent conference calls with sector entities, including the FSSCC, FBIIC, and the Financial Sector Information Sharing and Analysis Center (FS/ISAC), an organization that facilities communication and collaboration among financial sector firms on critical security threats facing the sector, providing the sector with advance notification of the pending threat level change, allowing the sector to rapidly strengthen security in and around specific buildings and locations as well as throughout the financial services sector.

Subsequent to providing immediate alerts to the financial sector regarding the threat, DHS's Infrastructure Protection (IP) Division continued to work with the industry to ensure that all targeted financial institutions were individually briefed. IP coordinated with Federal, State, and local law enforcement (LLE) entities to ensure that the appropriate information was exchanged between the government and the private sector. IP also polled the various financial institutions to determine what additional protective measures were implemented as a result of the heightened alert. This included the deployment of IP personnel to provide technical assistance, identify security gaps and provide federal resources to LLE and facility owners and operators.

Teams of IP personnel, in collaboration with local law enforcement officials and asset owners and operators, have conducted Site Assistance Visits (SAVs) to facilitate vulnerability identification and to discuss protective measure options. A total of 15 visits have been conducted thus far of facilities in the banking finance sector.

In addition to SAVs, IP personnel have been working with individual facilities and LLE entities to implement buffer zones around select banking and finance assets. The Buffer Zone Protection Program (BZPP) is a community-based effort focused on rapidly reducing vulnerabilities "outside the fence" of select CI/KR. To support these efforts, IP provides assistance to LLE officials to develop and implement buffer zone plans. To date, seven buffer zone plans for the banking and finance sector have been submitted to IP by State Homeland Security Advisors and are eligible for $350,000 in BZPP grants.

Based on data gathered from SAVs and BZPPs, DHS has developed five Characteristics and Common Vulnerabilities (CV) and Potential Indicators of Terrorist Activity (PI) reports for the banking and finance sector. CV/PI reports identify the common characteristics and vulnerabilities of sector assets and provide information on how to detect terrorist activity near critical sites. These reports have been distributed to all State Homeland Security Offices, with guidance to share these reports with the owners/operators of critical infrastructure and the law enforcement community within each State.

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

Protective Security Advisors (PSAs) are also stationed in New York City, Chicago, Washington, DC, San Francisco and other major cities with a large financial sector presence to represent DHS in local communities throughout the United States. PSAs serve as a liaison between DHS, the private sector, and Federal, State, local, and tribal entities and work to assess, prioritize, and secure critical infrastructure within a community.

After the August 2004 elevation of the threat level for the banking and finance sector, additional steps were taken to strengthen emergency preparedness and response by improving communications systems and protocols between and among financial regulators and critical financial institutions; assessing and reviewing business continuity plans; and participating in numerous drills and exercises to test backup systems and prepare financial professionals. These additional protective measures were permanent and sustainable enhancements that continue to be followed today, further reducing the possibility of attacks.

Improving Telecommunications Resilience

The financial services sector is reliant not only on its own resources and infrastructures to support its businesses, but also on several other key sectors, foremost the telecommunications and electricity sectors. This dependency on the telecommunications sector was the focus of attention in 2004, with several groups taking action to explore this dependency in much greater detail and to develop recommendations on how sector members can address and minimize it.

IP supported the development of the National Security Telecommunications Advisory Committee's (NSTAC) April 2004 "Financial Services Task Force Report." This report provided a thorough review interdependency issues and offered information and recommendations to the sector in addressing the diversity, redundancy, and recoverability

of its critical systems. DHS's Infrastructure Protection Division was represented on this work.

Protection and Enhancement of Telecommunication Capabilities

Over the past year, DHS has worked extensively to enhance telecommunications resiliency for the financial sector.

The National Communications System (NCS) conducted several activities which address the national goals, objectives, milestones, and key initiatives with regard to critical infrastructure protection as outlined in the NIPP. The NCS has worked with the Department of Treasury, the Federal Reserve Board (FRB), and other financial services institutions in the following efforts:

- **Development of the Route Diversity Methodology (RDM).** Route diversity (RD) is communications routing between two points over physically separate paths. The NCS developed RD recommendations for the FRB to enhance telecommunications resiliency for its Washington, DC location. Using the RDM, the FRB assessed the physical diversity and resiliency of its voice and data telecommunication systems. The RDM was also used to identify vulnerable assets and to develop mitigation strategies.

- **Enhanced Analysis Capabilities.** The NCS continues to enhance and expand its existing analysis capabilities, tools, and data sets to better assess the impact of various scenarios on the banking and finance community. The Operational Analysis Branch routinely provides the Information Analysis and Infrastructure Protection Directorate regional information identifying financial institutions' dependencies on the telecommunications infrastructure. Furthermore, the NCS recently conducted the Internet Disruption and Impact Analysis study to determine the reliance of various sectors, including the financial services sector, on the Internet in New York and Washington, DC, yielding results that identified critical service providers and assets.

- **Awareness of the Alliance for Telecommunications Industry Solutions' National Diversity Assurance Initiative.** On June 3, 2004 the Alliance for Telecommunications Industry Solutions' (ATIS) Chief Information Officers Council and the Federal Reserve Board agreed to form a partnership, known as the National Diversity Assurance Initiative (NDAI), to conduct an in-depth assessment of diversity assurance to the financial services sector including researching the feasibility of validating the existence of diversity on critical national security and emergency preparedness (NS/EP) circuits and identifying methods to assure that diversity is maintained on those circuits over time. Since the establishment of the NDAI and per its NS/EP mission, the NCS has maintained an awareness of the group's activities to remain informed on issues pertaining to national security telecommunications.

Homeland Security Information Network
The purpose of the Homeland Security Information Network (HSIN) is to provide a user friendly, secure and effective medium for the timely sharing of information between governmental entities at all levels (Federal, State, tribal, local and territorial), Private Sector organizations, and International partners. The HSIN system will also provide a secure and effective vehicle for collaboration among those entities, enhancing their combined effectiveness in preventing and responding to terrorist attacks and preparing for and responding to natural and man-made disasters.

HSIN-Critical Sector (CS) provides a common communications platform to encourage sector-wide planning, coordination, and information sharing. This platform will deliver an improved situational and operational awareness of the nation's critical infrastructures and key resource (CI/KR) sectors to both the public and private sector. HSIN-CS allows operators within a critical sector to share information in a secure manner with each other and with government and allows government to share its analytic capabilities and reports directly with a sector. HSIN-CS will be the primary tool for DHS to share security threat information with specific sectors.

HSIN-CS is being been deployed through the engagement by DHS with various Sector Specific Agencies (SSAs) and Government and Sector Coordinating Councils (GCCs/SCCs). Private and Public Sector owners and operations of CI/KR are encouraged to voluntarily participate on HSIN. Eleven HSIN-CS pilots have been successfully launched. Several more are in progress.

DHS will continue to explore the use of HSIN as a no-cost approach to reach 100 percent of the CI/KR sector members.

Conclusion

Since the threat level was raised on August 1, 2004, DHS in conjunction with Federal, State and local leaders as well as the private sector have worked hard to strengthen security in and around specific buildings and locations, and throughout the financial services sector. Today there are permanent protective measures in place that did not exist before August 1. These new measures include increased security at the affected buildings, enhanced screening measures, increased perimeter protection and the development of security buffer zone protection plans.

The financial services sector as also taken additional steps to strengthen emergency preparedness and response by improving communications systems and protocols between and among financial regulators and critical financial institutions; assessing and reviewing business continuity plans; and participating in numerous drills and exercises to test backup systems and prepare financial professionals.

DHS remains dedicated to working with infrastructure stakeholders across the country to increase the security and protection of our Nation's critical infrastructure sectors. Thank you. I would be pleased to answer any questions you may have at this time.

Mr. PLATTS. Thank you, Mr. Caverly. Mr. Muccia.

STATEMENT OF DANIEL MUCCIA

Mr. MUCCIA. Thank you, Mr. Chairman, and Congressman Towns for allowing me to submit this testimony to you today on the current status of financial market preparedness for wide scale disasters or disruptions.

I will briefly summarize the key points contained in the department's written testimony. First, I do not believe that the financial regulatory community or the banking industry have become complacent. The stakes are too high, and the reminders too frequent. Certainly, if there was a threat of complacency setting in, the recent catastrophe in the Gulf Coast and New Orleans has served as a powerful reminder that we can never be too prepared.

Second, effective communication and coordination between State and Federal banking agencies is essential to rapid recovery. From our perspective, the protocols set in place by the Financial and Banking Infrastructure Information Committee, which Mr. Parsons chairs, or FBIIC, have proved to be effective in improving communication and coordination. We understand from our fellow State regulators in Louisiana that coordination with their Federal counterparts in response to Katrina have been excellent. We at the New York State Banking Department know how valuable that communication and coordination is, as it was tested both during September 11th and the August 2003 power blackout. Third, our assessment of the readiness of the New York State banking institutions we directly supervise is based on our ongoing supervision and onsite examination programs. Overall, our examiners are giving good grades to our institutions. The small number of institutions that are considered critical to the system are being held to a high standard of business resumption capability and are expected to meet current supervisory standards and targets. The vast majority of noncritical institutions have adequate plans and those missing the mark are in the process of correcting deficiencies.

One area that we will be focusing on in the near term is testing. More testing of business continuity plans is needed. Test results need to be more carefully and vigorously audited and the scope of testing needs to be widened. We are discussing how to achieve this with the Federal banking agencies that share our supervisory responsibility over our institutions, and I expect formal guidance will be issued in 2006.

Finally, we recognize that business continuity planning is a continuous process that requires our constant vigilance and attention. We are committed to insuring our institutions are as prepared as possible and thank Congress and this subcommittee for your continued support and attention to this critical challenge. Thank you.

[The prepared statement of Mr. Muccia follows:]

TESTIMONY OF

Daniel A. Muccia
First Deputy Superintendent of Banks

New York State Banking Department

Before the

House Government Reform Subcommittee

Government Management, Finance, and Accountability

September 26, 2005

Thank you Chairman Platts, Congressman Towns, and members of the Subcommittee for asking the New York State Banking Department to report on the current status of financial market preparedness for wide-scale disasters or disruptions.

The New York State Banking Department is the regulator of more than 3,400 financial companies operating in New York State. This number includes 165 state chartered commercial banks and thrift institutions and 111 U.S. branches and agencies of foreign banks. The aggregate assets of these supervised entities total nearly $1.3 trillion. The Department also licenses, supervises and regulates a total of 3,100 mortgage bankers, mortgage brokers, check cashers, money transmitters, licensed lenders and budget planners.

Since the tragic events of 9/11, the financial services sector has been on a steady march of progress towards strengthening its preparedness for disasters. The resiliency demonstrated after 9/11 and the August 2003 power blackout in the northeastern United States and Canada was truly remarkable, however we cannot afford to be complacent and I do not believe we have become so. If there was a threat of complacency setting in, the recent catastrophe in the Gulf Coast and New Orleans caused by Hurricane Katrina should serve as a horrible reminder of the need for continuing emphasis and attention to business continuity planning and testing. One thing is certain, it is impossible to be too prepared.

Coping with wide-scale disasters or disruptions, whether man-made or acts of nature, will always be difficult as the destruction that ensues taxes societies' normal expectations of public health and safety and order. Financial services providers do not after all live in a vacuum. They are your neighbors, they have families. The first rule in any disaster contingency plan is to provide for one's own safety and that of one's family. Business recovery plans come second and must account for the safety of employees and data simultaneously. At the local level, first responder agencies are critical to personal and business survival, rescue and recovery and need Congress's support. While much has been done to better supply and support local disaster teams, more emphasis on this critical function is needed.

Putting the health and safety issues aside, the Banking Department believes much progress has been made in disaster planning by the financial services sector. Systemically critical organizations have made substantial progress in improving their resilience and achieving out-of-region geographic dispersion between primary and backup facilities. These organizations are being held to a high standard of business resumption capability. All banking organizations are expected to maintain a level of resilience appropriate to their role in the marketplace.

The Banking Department believes that Congress can be of most assistance to the financial sector by supporting efforts to improve the resiliency of the power, water, transportation and telecommunications infrastructure upon which the financial sector relies.

The Banking Department plays an important role in assuring the banking industry in New York State is ready and prepared.

First, our most important function during an emergency is to act as a conduit of accurate information to state and federal senior policy and emergency officials about the status of the industry. To do this efficiently, we are an active participant in disaster recovery efforts on the local, state and federal levels. On the local level, we communicate and coordinate with the NYC Office of Emergency Management ("OEM") and have established communication protocols. In the event of a disruption in New York City, as part of the Banking Department contingency plan, a senior member of our staff is assigned to NYC's OEM operations center.

On the state level, the Banking Department is a member of the Disaster Preparedness Commission and coordinates activities with the State Emergency Management Office ("SEMO"). Banking Department staff regularly participates as needed in contingency drills conducted by SEMO. The Banking Department's contingency plan includes assigning staff to the SEMO operations center in the event of a disruption in NYS.

Immediately after a disruption, it is our protocol to consult with the Governor's office to assess the situation and to request an Executive Order declaring a bank emergency or holiday if necessary. Working with SEMO and our fellow federal regulators, we help deliver emergency services to affected institutions, assist in the delivery of cash or other needed banking services, answer consumer inquiries and advise the Governor's office on the status of our financial institutions.

On the federal level, the Banking Department, working through the Conference of State Bank Supervisors, is an active participant in the Financial and Banking Information Infrastructure Committee ("FBIIC") which has established a protocol that facilitates the sharing of information among the federal financial regulatory agencies, state financial regulators and others responsible for promoting the financial integrity and soundness of the financial services industry. FBIIC is chaired by the Department of the Treasury. Senior Department staff regularly attends FBIIC meetings and supports FBIIC efforts as needed. These protocols have proved valuable even in the events that have not directly affected New York State. For example, earlier this month we responded to a request for a public communications expert to assist the state of Mississippi which had been circulated through FEMA and SEMO. In addition, Department personnel are staffing a Harlem facility opened by OEM to assist Hurricane Katrina relocatees.

Secondly, through our regular on-site examination program for all our regulated entities, we are actively monitoring the status of business continuity plans and readiness at our regulated institutions. Department examiners use the Business Continuity Planning IT Examination Handbook issued by the Federal Financial Institutions Examination Council (FFIEC) when conducting such examinations and reviews. The examination procedures are designed to determine whether the institution has an appropriate enterprise-wide business continuity plan that covers all business units and functions and that it is kept current and frequently updated. Examiners are instructed to determine:

- the quality of oversight and support provided by the Board of Directors and senior management;
- if adequate business impact analysis and risk assessment have been completed;
- if appropriate risk management over the business continuity process is in place;
- whether the plan includes appropriate levels and frequency of testing;
- whether the IT Business Continuity Plan properly supports the goals and priorities of the overall business unit plan;
- whether the appropriate hardware backup and recovery is maintained;
- whether the process includes appropriate data and application software backup and recovery;
- whether the plan includes appropriate preparation to ensure the data center recovery processes will work as intended;
- that the appropriate security procedures are included in the plan; and
- whether the plan addresses critical outsourced activities.

Examination findings and recommendations are formally communicated to senior management and if appropriate the Board of Directors. Corrective action plans are monitored by our examiners until resolved. If necessary, informal and in rare instances formal enforcement actions are taken to address serious deficiencies.

Results of the latest cycle of on-site examinations are satisfactory. While not every institution's business continuity plan meets all the supervisory expectations, the vast majority of institutions have developed adequate plans and/or are in the process of correcting deficiencies. Weaknesses most frequently cited by examiners relate to insufficient testing both as to coverage and frequency and inadequate independent audit or verification of test results. In a small number of non-critical institutions the plans are simply not comprehensive enough.

Critical and significant institutions have made significant strides in obtaining geographic diversity for critical functions. For many non-critical institutions primary and back-up sites tend to be within a relatively limited geographic area that could conceivably be simultaneously affected by a large-scale event. While this could hinder the speed of business resumption and recovery for these institutions, it does not pose a systemic risk to the financial system and is considered adequate under the current supervisory standards and reflects a reasonable risk and cost-benefit analysis. We mention this simply to note that it is, of course, still possible that some institutions and their customers in individual cases could be inconvenienced in the aftermath of an event of significant force and geographic reach.

In conclusion, the Department is committed to ensuring that the institutions it supervises are as prepared as possible. We will continue to work with local, state, and federal agencies to seek practical solutions. We fully understand that business continuity planning is a continuous process that requires our constant vigilance and attention. This is best achieved through our on-going examination and supervisory process.

Mr. PLATTS. Thank you, Mr. Muccia. I appreciate each of your testimonies. Each of you I believe in your written testimony and here today referenced an August 2003 blackout. It was in a sense the first major test after September 11th here in the New York area. The blackout was also a test especially throughout the northeast of how our new coordination was going to work. I'm interested if each of you would want to share your perspective of how your organization responded. Also, what will be especially informative is the things that didn't go as you expected 2 years after September 11th.

Mr. PARSONS. Sure. Our observation is, as you noted, Mr. Chairman, the power outage was indeed the first real test of the mechanisms that we put in place after September 11th. We felt they worked very, very well for a couple of reasons. One is it was critical to get information out to the sector as quickly as possible, and it had to be an exchange of information. We knew there was a blackout, but we also wanted to find out what was happening in New York City.

Those mechanisms worked very well. The communications that we had built in were very effective in ascertaining the situation and within 15 minutes or so we had a good understanding of what exactly was going on. I would also note that they were instrumental in being able to help spread the word as quickly as possible. This was in fact not a terrorist incident, which I think was very, very important for everybody at that time to understand.

Additionally, it enabled us to convene, for example, all of the financial regulators to look for any problems that we may have had. If there were any imbalances created due to the time of the incident, thankfully it came after the closing of most of the major markets. Were there any things or actions that we needed to do to immediately from a regulatory standpoint, and then also in working with our private sector coordinating body, the FSSCC, we were able to identify any needs that they may have had very quickly.

I think it's important to note that the financial sector is extremely resilient and most of the firms here have well-drilled, well-thought-out backup emergency plans.

Nonetheless, we used this mechanism to find a couple of examples where we needed to intervene. One example of that is at the American Stock Exchange. It needed a new generator so they could cool its training floor. While working with the New York Office of Emergency Management, we were able to coordinate the delivery of that to help the AMEX get back on line quickly.

Very briefly, I would say there were some lessons learned for us. One of them is the interdependency that we have on other sectors. You heard Mr. Caverly talk about telecommunications. That's a very big concern for us in financial, but we also learned, for example, the need to resupply generators to—if we were going to have a sustained outage, and we have subsequently through the FSSCC convened meetings with other government agencies like the Department of Energy and the Department of Transportation to discuss these and other lessons that we learned not only from that event, but from other pieces of our thinking on this as well.

Mr. PLATTS. Thank you.

Mr. CAVERLY. One of the things that it did was reinforced the critical role that information sharing plays. There were existing mechanisms prior to the creation of the department; relationships between telecommunications and electricity specifically because of their interdependency nature. Based on the activity that came out of that, DHS has set up the National Infrastructure Coordinating Center, to provide transparency. The lesson that moved us in that direction was that on Friday morning after the blackout, as we were talking to the telecommunications and electricity people, the electricity people pointed out that power would not come on in Detroit until Sunday. The telecommunications people identified that presented a significant program for their wireless nets, because most of them depended on batteries, some on generators. They recognized they needed to bring more generators in as well as resupply the fuel to the generators that were there, but they didn't have existing relationships with suppliers.

We were able to take them and connect them up with the Michigan State Energy Office who knew all the suppliers and could quickly make sure they had the supply they needed until the power came back on.

It's that kind of transparency and sharing of information that's critical to a situation like that. The media gives us some heads up, but there are things that come from the operating parts that the owners and operators know and we need to create a better more fluid forum. The NICC is the process, and as we built the connectivity it provides the capability for those extraordinary communications that have to take place in a crisis.

Mr. MUCCIA. I would agree with Mr. Parsons in terms of the overall connectedness of communication. I think one of the things that happened was some of the protocols we put in place that we learned sort of ad hoc on September 11th we got to use in the blackout event. It was a more formal structured way of communicating that helped get the word around more quickly. Our institutions did very well.

So overall in our department we exercised our plan and had representatives at the Federal Reserve in New York. We were in contact with SEMO and New York OEM. So overall, it worked very well.

Mr. PLATTS. The lessons learned in that coordination, for example, the fuel to the generators to control and identify quickly what the problem was, how did working with utilities, what was the cause for that? I think you're right to get the word out quickly to the public that this is not a terrorist attack. It was a infrastructure breakdown basically. I didn't learn it as quickly as the rest of the country, because I was tent camping in the Northwest at the time. I learned about it a day late I think, behind everybody else. I was removed from civilization with my wife and kids.

But in getting a handle of what did happen and how quickly word did get out, given that the utilities are private sector, how did that happen? You needed to learn here's what happened, why it happened and then share that publicly.

Mr. PARSONS. The first thing we determined very quickly is that this is not an act of terrorism and that was simply done by—I

guess it would be a collection of information that flowed in all at once.

Mr. PLATTS. Was it the private sector coming forward too?

Mr. CAVERLY. It was.

Mr. PARSONS. Both.

Mr. CAVERLY. To some degree you can understand the structure—the North American Electrical Reliability Council, which sets the reliability standards for the electric industry is a central point for information. They were on the phone by 3:30 that afternoon identifying the cause of it, which was a rolling blackout caused—they didn't know initially what caused the system to start tripping out, but they were able through their reliability coordinators in the reliability region to identify that's how it happened. Then you went back to the operating center. So they built the picture quickly of what the cause was, being able to talk.

So the information comes out of them very, very quickly into the system. Remember, it is a regulated industry, so the reporting requirements are a little more structured than some other parts of the private sector. In that case the information came out of it, as well as the reporting you were getting in the media—there was no report of explosions or other such things.

Mr. PARSONS. Mr. Chairman, it was also useful again to hear from people in the affected city who were saying, "we don't see any explosions, we just see the lights have gone out. There's no smoke, there's no fire." I guess I would answer that it was kind of information flow both ways, to and from.

Mr. PLATTS. Mr. Muccia, you mentioned that you worked with SEMO here in New York. Would that have been the case prior to September 11th, your involvement, the Banking Department, immediately, being part of that Statewide effort in responding? Did that change because of September 11th or would that involvement of the Banking Department be there already?

Mr. MUCCIA. It really changed I think to a significant degree with preparations for Y2K, where we really—we always had it there, but I think in terms of taking it more seriously and being more prepared, it started with Y2K and certainly September 11th really brought it home.

Mr. PLATTS. Obviously, there's an endless list of efforts we could engage in and you've each highlighted some very important ones that your organizations are now pursuing. There's not an endless sum of money out there, and so you need to be smart.

Last, we had a hearing on managerial cost accounting in trying to make that cost benefit analysis on the Federal level in that case in two or more departments; Veterans Affairs and Labor. In what way does that go on with your respective organizations that you're trying to do that kind of cost to benefit? It kind of relates to the Commissioner, the threat-based provision of funds, but internally in your organization, how do you go about that?

Mr. PARSONS. That's a very good question. We do have a limited sum of money and as you noted, we could spend freely, but we can't do that. So what we try to do is we try to take a risk-based approach to our efforts at the Department of Treasury. What we've first done is working with the other financial regulators, we've identified the wholesale clearing payment system, which is really,

if you really think about it, it is the series of mechanisms and institutions that really make the financial system work, and we've chosen to direct our efforts to those entities, believing that we will get a huge return that will in fact create a cascading effect and that other firms will benefit from this knowledge and our efforts there.

We've embarked on a testing regime which is not focused on simply doing a test, it's really focused on doing a plan, and that plan involves the State and local officials and the affected institution, the institution that we've all collectively identified or the series of institutions. So it's very targeted and at the end of the day we have a plan that not only involves one center, but involves many of the operating capacities within these given institutions.

So I guess I'd summarize by saying you really have to take a risk-based approach in thinking about where will we get the best return for our dollars, and we do think about it before we accentuate programs.

I would also add through our partnerships with the regulators and with the Financial Services Coordinating Council we get a tremendous scale to our investment and it reaches a vast majority of the financial sector.

Mr. CAVERLY. Secretary Chertoff is devoted to a risk-based approached in vulnerability and consequences related to the infrastructure. As you can imagine, the department has to look across all 17 critical infrastructure sectors. The RAMCAP methodology that I mentioned earlier allows us to look at the risks associated across the sectors and ultimately prioritize and allocate across the sectors the limited resources that are available.

It doesn't do us particularly good if you have the best and most resilient systems in the financial services sector and you haven't accounted for the risk to transportation or telecommunication risk or cyber risk. So we have to look across all those components of a very intertwined infrastructure and prioritize our assets on a risk basis, so in fact we make the system resilient.

Mr. MUCCIA. We also use a risk-based approach in terms of our supervision and examination and key to that is really our program of CPC's or resident examiners at critical institutions that we share responsibility with the Federal Reserve or the FDIC, depending on the institution. So we leverage off each other in terms of sharing resources, responsibilities with the Federal banking agencies and we use resident examiners on those key institutions to stay in touch and in focus and we leverage off work. We can't do it all ourselves, even the Federal banking regulators can't. We leverage off the work done by the businesses themselves, utilizing their internal audit reports and their external audit reports and their internal policies and procedures.

Mr. PLATTS. You mentioned in your answer about RAMCAP. Where do we stand in that development deployment of that?

Mr. CAVERLY. The framework for the methodology has been developed across the spectrum. We are now doing modules across each of the sectors. Obviously, that methodology is important as we develop the NIPP plans for each sector-specific agency. So those are scheduled to be completed later this fall for each of the sectors.

Mr. PLATTS. Thank you. Mr. Towns.

Mr. TOWNS. Thank you very much, Mr. Chairman. Let me begin with you, Mr. Parsons. You talked about a regional coalition and of course you talked about ChicagoFIRST. Many people are saying that methodology should go further than Chicago, because there's extra cost involved.

My question is, ChicagoFIRST, I thought it should be New York First, but that not being the case, could you tell us in terms of the makeup of that and what it's all about and is it true that the reason you're having difficulty moving it forward is because of the additional resources that would have to be allocated in order for it to be a reality.

Mr. PARSONS. Congressman Towns, I can tell you, ChicagoFIRST is an interesting story. It started out with two participants for large firms there who said, hey, we feel like we're not getting adequate representation to the local level, at the local level for what the financial services sector really needs. And that conversation led to an idea which in turn led to collaboration and the result of this over a period of time, including with the encouragement of the Department of the Treasury was the establishment of ChicagoFIRST.

I can comment on a couple of things related to funding. One is, it is a self-funding organization. That is, its members have agreed to pay dues to fund its effort. They have appointed an executive director who is a full time employee and who coordinates all of their activity. They also have a president and they have a board of directors that oversees their operation. So I don't believe that in the case for ChicagoFIRST that funding has become a tremendous issue at this moment in time.

What I would add, though, is we've been working actively to encourage the creation of other organizations like ChicagoFIRST in other areas of the country, and we believe they're extremely useful. I would note it would have been very helpful, for example, to have sort of a single point of contact that represented the financial services sector in New Orleans as we worked for the recovery of Katrina. I think our mechanisms are working well. This would have simply augmented and made our flow of information and our exchange of needs and ideas more effective.

So we are hopeful that we're going to have, in fact, we plan on having an announcement on October 13th about the formation of a new organization in Miami. We hope to have additional organizations as well.

Mr. TOWNS. Let me ask you, will you provide additional money or resources to move this forward? I know you said there's the different companies, agencies put money in, but are you willing to also put additional resources in in order to make it a reality?

Mr. PARSONS. That's a great question. We at this time, we have not planned for specific investments toward the establishment of these organizations, other than our work to go down and share with them the documents I referenced in my opening remarks and written testimony that we partnered with BITS on, a how-to model, a how-to cookbook, if you will, to establish these organizations.

What we have done, though, and we've done this twice with the case of ChicagoFIRST, is we have funded an exercise with ChicagoFIRST as the point to test various aspects of response, recovery and generally trying to identify needs within the commu-

nity, and I would tell you that we would plan on doing that for the other regional coalitions as well.

Mr. TOWNS. There seems to be a lot of excitement around ChicagoFIRST. I just want to share that with you. I think that's important.

Mr. Caverly, as the department moves forward with its reorganization under Secretary Chertoff, can you describe for us how the new structure of DHS will improve the agency's efforts to strengthen critical infrastructure protection activities? Will these new government structures have adequate authority and attention from the Secretary? How do you anticipate the new Office of Intelligence and Analysis improving upon the sharing of information between public and private sector participants, such as the financial markets?

And also, I guess in terms of the issue of privacy, has that popped up?

Mr. CAVERLY. Let me answer the question somewhat in a bit of reverse order. On the privacy issue, privacy always remains a critical concern of the department, because as you look for the information that will help you do—identify the strengths, identify indications and warnings, we always run into the risk of having information on U.S. citizens that cause problems with existing privacy laws. So we're working very, very hard to insure that we get a robust information analysis system that doesn't violate the rights and privileges of the American citizens for the privacy of their personal information.

So we work at it. It does present certain problems that each of the units within the department have to work with based on the kinds of information they need to build the picture that allows them to assess risk, identify threat.

Relative to the Secretary's reorganization, I think if you look at it, the new rules proposed under the Secretary for preparedness if you think about it, protection is a seamless framework that goes from preparedness through protection to response and recovery. Because if you can respond and recover as quickly and efficiently as possible, you reduce the impact, reduce the consequences of an event, whether a natural event or man-made event, terrorist event. So what the secretary has done in that case is combined into one unit the responsibility for the preparedness which the administration recognizes in HSPD8 the responsibility for protection or prevention, if you want, in HSPD7 and the response and recovery which is in HSPD5. So he brings together a framework that has both the preparedness planning, the infrastructure protection planning and, obviously, the national response plan all into one framework.

The other thing I think that the Secretary's reorganization recognizes is there's a vast span of responsibilities in agencies of the department, and what he's really set up is a framework that allows the coordination and the sharing of information and the transparency necessary so that those various responsibilities resting with individual agencies and organizations can complement each other and not duplicate.

Mr. TOWNS. Right. Thank you very much.

Mr. Muccia, let me ask you, sharing information about potential threats is viewed as a critical step in helping to insure the financial institutions are better prepared to protect their operations from disruptions. How is your organization assisting in providing such information to financial institutions? I would assume that an electronic attack could easily be targeted on a small institution just as it could a larger one. Are there additional barriers you can identify for us in regards to effective information sharing practices that are the potential solutions to this problem?

Mr. MUCCIA. Thank you, Congressman. You mentioned cyber attacks and New York has a cyber security office that concentrates on those threats and gives advice to the industry, and one of the mechanisms we actually have set up is a collection of those types of events that gets centralized at the New York office and then scrubbed of identifying information and then put out to the industry so they're aware of what types of attacks are going on.

In terms of information sharing, in terms of a crisis, we have a number of points of contact, where we will establish communications. One of them I already mentioned before, that is indeed our resident examiners at individual critical institutions. For all institutions, including the small ones you talked about, we have numerous contacts available to them. Obviously, they kind of depend on the telecommunication system working, but we have obviously contacts through cell phones, Blackberry, we have some satellite phones available to the department, so in terms of the infrastructure we have as many different varieties; Internet, available.

If our offices in New York City—and we will reach out, part of our plan is we like to be proactive and reach out to institutions to find out what's happening—if we're disabled in our offices downtown, we switch to our offices in Albany. If we need to reactivate our hot site within 24 hours, if we have to do that, we have numerous points of contact. We also have examiners who have given their contact information, their home phones and so forth to various institutions, so we have a number of ways of doing it and then with our programs of having representatives at the State Emergency Management Office at their operations center, at the New York City OEM office and at the Federal Reserve Bank of New York, we therefore have numerous points of getting into contact.

Mr. TOWNS. Thank you very much. Let me just ask all of you down the line, starting with I guess you, Mr. Parsons. You always hear about communications, sharing of information, coordination, you always hear this. Is there anything that Members of Congress can do to improve or facilitate that in any way? I know you guys hate for you us to stick our nose under the tent, I understand that.

Mr. PARSONS. Congressman, that is truly an excellent question. You know, we've put a lot of effort, as you noted, to information-sharing mechanisms. I would note here today that Director Caverly is working very hard on the further creation of the Homeland Security Information Network, which we wholeheartedly support and we think that's going to be an excellent mechanism. It will complement other things that we have currently in place.

Honestly, I think at this point I don't have a good answer for you, other than to say nothing comes to mind.

Mr. TOWNS. Right, OK, thank you.

Mr. CAVERLY. Congressman, I think there are two things. One is something, not something Congress can fix, but is just getting the two institutions, government and the private sector to understand the information needs on both sides and be able to transfer them into something that's useful to them. The intelligence community presents information in a certain way that is understandable to professionals that have dealt with them for a long time, but not potentially understandable to a security director who has not been engaged with them for a long time. Our job is to find ways to do that and we're working very much on.

I think the other issue, I think this is one where the legislative entities across the country, whether they're local, State or Federal, need to continue to search for the right balance between the need to have sensitive information protected so that it's not in the public domain versus the public's right to have the information it needs to form judgments. There's a delicate balance, but we're moving into an area where the information needs to be shared between the owners and operators, the infrastructure and the government, that doesn't need to be in the public domain, whether it's vulnerability information or intelligence, and we need to strive to find a balance in those two very pressing needs.

Mr. MUCCIA. Congressman, nothing comes to mind right away. I think in my limited world of banking supervision we've had a long history of cooperating with the Federal banking regulators, State and Federal, through our joint examination programs our joint supervision programs, so we're very used to having this close coordination and communication.

Mr. TOWNS. Thank you very much.

Mr. PARSONS. Congressman, I just might add, Congress has already acted in a very beneficial way, that's the Intelligence Reform Act; working to bring down barriers between agencies that will help us to share information both among ourselves and with the private sector as well.

Mr. TOWNS. Thank you. I yield back to the chairman.

Mr. PLATTS. Thank you, Mr. Towns. Mr. Parsons made specific reference to the Patriot Act, intelligence reform. We're obviously dealing with the reauthorization of that and trying to strengthen some of the civil rights protections, but as I referenced to Commissioner Kelly, that information sharing, obviously, is critical to what you do within the Federal department or in sharing information with local entities like NYPD.

Mr. PARSONS. Yes.

Mr. PLATTS. I want to ask Mr. Caverly, you in talking about the Infrastructure Protection Plan, that implementation going forward, how often is that coordinated plan reviewed for—in response now to Katrina and Rita, how would that process go forward? Is it a weekly review, monthly review? Is there a set approach to it or is it more just as we learn you go back and revise?

Mr. CAVERLY. I think there are several pieces of that. There is a preparedness plan, which we've begun to work on with the department relative to the scenarios to be prepared to deal with and that's an iterative process that the Office of Preparedness will be doing.

The National Infrastructure Protection Plan is still under development. We have a base plan framework that we put out an interim plan last February. The base plan will come back out for comment to the American public shortly. Then there will be individual sector plans after that.

Currently the plan is for the Director to look at that annually. We may look at that cycle and say maybe a biannual review, it might be longer than that. Then ultimately the response down to Katrina and Rita were all carried out under the National Response Plan, which was an effort by the department based on congressional direction to combine a large set of Federal response plans that were not connected in a single framework. So the National Response Plan put out a year and a half ago does that and that will be a process to come back and see how well those integrated pieces work down in the southern part of the country.

Mr. PLATTS. In developing the plans and getting feedback on how to protect the infrastructure, and today we're focused mostly on the financial sector, but another part of infrastructure is chemical facilities, chemical plants. How much outreach—I'll give you an example. I had a constituent came to me and my staff, then followed up with the department in terms of how this was being addressed. A driver for a company that does a lot of transportation of chemical, very volatile chemicals and his concern that when presented with some of these plans, the identification, confirming that he is who he's supposed to be and entitled to pick up this very volatile supply order, that it was very lax.

Do you reach out within the department where actually you go to those drivers and randomly pick some; say, how do you see it? Or, how do you get feedback?

Mr. CAVERLY. It's a couple of things. There's obviously security protection advisers located around the country going out to facilities, visiting the supply chain part of those facilities to pick up that kind of information.

Across something like the chemical sector, there's a range of activities they do from something like the American Chemistry Council for the largest manufacturers that have a responsible care program for their security program, which is best practices for them. Some of the other groups do. We created a Chemical Sector Coordinating Council along the lines that we've seen in financial services for the intent of making sure that those kind of best practices, those kind of knowledges, those protected activities can be translated across a wide range of different kinds of facilities, different kinds of concerns and operational realities.

I think it's a mix of the two things you identified.

Mr. PLATTS. I would encourage that outreach in that example that the driver, his—as we're doing more background checks on the drivers so they can get their license and be approved. Say it doesn't mean a whole lot if someone bumps me off enroute, takes my spot and pulls in and they don't check to see he's not me. That type of outreach. Sometimes we look at that big picture and forget that the guys are in the front lines, get their insights which are sometimes——

Mr. CAVERLY. That highlights the interdependence of all of the components. It's not just a single component. It's a system of systems.

Mr. PLATTS. It is. You have to look at the plan itself with the transportation network that's involved in distributing what that plant is manufacturing.

Mr. Parsons, on the interagency capability sound practices to strengthen the resilience of the financial system 2006 timeframe we're looking at for those protocols or those practices being put in place, what's your assessment of where this industry is as being able to comply with that timeframe?

Mr. PARSONS. I believe the industry is well along, and I believe they will comply with deadlines that have been set.

Mr. PLATTS. Is there any possible problems that may need to be revisited or just that are not realistic or overall, are you optimistic?

Mr. PARSONS. Congressman, at this point I've heard of no problems, I'm not aware of any. So we remain optimistic the goals will be met. I will take the opportunity to commend the sector because they have been extraordinary in their response to this document and they've made extraordinary investments and extraordinary progress.

Mr. PLATTS. Great. The coordination. And Mr. Caverly this may be specific to you, the coordination, again, of information being shared here, it seems that we've seen tremendous success in the private sector and public entity in sharing information, what's happening and how we need to respond. We had a blackout in York—old York, PA, not New York—a while back and one of the issues that came to my office was there wasn't a preestablished ability of businesses to have direct access to utilities. Where all of us as residents want our refrigerators working, our lights on and air conditioners individually, but there are entities that affect a much greater population base because of the service they provide to the private sector, and so they ended up coming to me, because I had a contact through my State House days in dealing with this utility and we kind of became the conduit for information from the utility, the private sector provider and timeframe to these businesses, especially food warehouses and things, so we could decide how are we going to manage this problem long term.

We became that conduit. Obviously, it would have been better if it was preestablished. What do you hear on that direct access specifically to the energy, to utilities with the financial sector in New York?

Mr. CAVERLY. I think in New York, again, based on the history that the financial sector has had with New York, it has very good connectivity both in telecommunications and electricity. Again, unfortunately it's because they had problems in lower Manhattan historically that did in fact move this up on the many things that somebody has to consider in assigning their resources to.

I think what you highlight is the need to say one size doesn't fit all here; that we need things that operate on a local level, could operate on a regional level and could operate on a national level to insure that the kinds of information that you need to continue your operation, the continuity of operations, is accessible to you.

The utilities are doing a much better job in putting information now up on the web and having it accessible, but, again, if you're not used to looking for it there, it might take you some time to find that information. They understand the benefit to them of having that transparency out there and being able to get the information out, particularly in a day of 7 by 24 news coverage where, clearly, misinformation causes far more trouble frequently than not. So there is a incentive for them to provide that kind of connectivity.

If you look at groups like ChicagoFIRST, if you look at the program that Commissioner Kelly talked about Apple in New York, those local activities that provide that connectivity and dedicate the time to be connected to understand where to get that information is a thing that has to happen. So I think we all have a role to play in getting to what you're suggesting, which is the ability to have the information needed to make the decisions when something happens.

Mr. PLATTS. And that's great for a followup. When it's information from your organizations to the private sector, some of that information is very sensitive intelligence information. How do you handle or prepare for the transfer of sensitive intelligence with those receiving entities? Do they go through a certain level of personnel background checks and things that they're entitled to be privy to to what you're sharing?

Mr. CAVERLY. Unfortunately, the system that we have for protecting that national security information never envisioned what we have now, which is part of the private sector, we have been able to through a system of security clearances, etc., create a framework in which we can get information to them. It's not as efficient as we'd like. Homeland Security Information Network, as we develop the capability and adjust the flow of information, ultimately I think will allow us to get information to the owner operators in their place of decisionmaking. Right now it's pretty awkward, because we have to bring them into a classified facility, assure they have a clearance, but one of the things we're looking at is how can I be sure I can give you quickly timely the information you need to make that decision at the place where you need to make it, because if you don't, we can't be as efficient as we want.

Clearly, with the financial institutions in New York, their leadership all have security clearance. We were able to work very closely with them in sharing some of the most sensitive information last August, because we knew the need of being able to share it with them. But we were able to do that on an ad hoc basis and I think we need to move to a much more systematic capability. But it requires changing our whole framework for protecting sensitive national security information that's been in place for a long time and that takes a lot of time.

Mr. PLATTS. In that review, that's something the department is engaged in, how it's going to try to streamline that?

Mr. CAVERLY. How to streamline that, how to make sure the information can go to someone who has to act on it in a protected way without it becoming cumbersome for them to have to receive the information.

Mr. PLATTS. Thank you.

One final question, Mr. Muccia, that in your testimony you talked about the review of the Institution Business Continuity Plan and the importance of the board of directors' senior management being engaged in understanding and appreciating the importance of this issue.

In those reviews, what is the norm? Is it the norm that the senior board members and executives understand that continuity disaster recovery is critical in today's time that we now live in? Is that the norm, or are there some that still don't get it?

Mr. MUCCIA. Mr. Chairman, that is the norm today. I once had a mentor who told me the key to success in business was if your boss was interested in a topic, then all of a sudden you become extremely interested in that topic, and I think now the events that we've had in the past and the examination programs that we've have that really lie responsibility at the very top with the board of directors. They know that we'll be taking enforcement actions against them if they're not paying attention. They have paid attention and have pushed down that message to senior management and have held them accountable. That's where we see success. When the board is active, when the board knows the plans, when the board is monitoring the status of those plans; that's when we've had success with the institutions. We've had some smaller institutions that still have some work to do, but we are working with the institutions to make sure they get the message.

Mr. PLATTS. I would share the message with your mentor. Those are some wise words. I learned from my mom and dad. If my mom or dad was focused on something, it was important for me to get that done.

Mr. Towns, do you have any comments?

Mr. TOWNS. I just hope my staff is listening. I do have one more question. I'd like to direct this to Mr. Scott Parsons.

Treasury released a report that essentially called for the ending of the terrorism insurance backstop for insurance to provide terrorism insurance products to the marketplace. Many industry participants, including some of those before us today, have called for extending the authorization of such programs.

Can you describe for us the economic incentives or barriers that are present in today's market to justify such a decision? Won't the loss of the TRIA backstop provide less incentives for insurers to private such coverage?

Mr. PARSONS. Congressman, I appreciate the question; appreciate the spirit of the question. My response to you is the department did issue a report and Secretary Snow has signed it and would I let that report speak for the position of the department at this point.

Mr. TOWNS. No further comment?

Mr. PARSONS. No, sir.

Mr. TOWNS. Well, I can understand the sensitivity about it, but you also need to understand our concerns.

Mr. PARSONS. Certainly.

Mr. TOWNS. We'll drop it at that.

Mr. Chairman, I'll close on that note, hoping, though, we could get some kind of written response from the Treasury Department, because this is something that we have people asking a lot of questions about and we can't give them the answers, so I would appre-

ciate that, recognizing you might not be prepared to do that this morning. We look forward to getting that. Mr. Chairman.

Mr. PLATTS. Exactly, Mr. Towns. I would suggest if the department will followup to the committee in writing, we'll keep the record open for about 2 weeks for that submission.

I want to thank each of you. I did have one final question in a broad sense, because we certainly as fellow Americans are watching the devastation of the Gulf in recent weeks now with Katrina and now Rita. We also appreciate in trying to help those citizens and businesses recover the tremendous demands on the Federal, State and local private sector. You read on how that's going to impact your department and ability to continue all the other efforts that are underway in Homeland Security, at Treasury and to have your arms around the needs of the Gulf Coast, is there anything you want to make sure we're aware of that's going to be challenging for your departments?

Mr. PARSONS. I would just make a general comment, Mr. Chairman, which is—it has been a very taxing month, and we have worked very hard to make sure that the people who have been affected by these storms have financial services that they need to conduct their lives, and I have to tell you I have seen some extraordinary work done at all levels; at the State level, at the local level, at the Federal level, and especially the citizens and business owners who are down there.

What I would just tell you is that it has opened a new set of thinking for us in terms of lessons learned, in terms of things that we think we need to be doing as a next step in preparing the financial sector, so we anticipate a real effort to get some good lessons learned out of this, but not just to have lessons learned, but to actually act on them and make sure. It's our philosophy that we need to make sure we understand what is happening and be better prepared for the next one.

Mr. CAVERLY. I think two things. The Secretary's reorganization saw the need to insure that we had a better balance between the preparedness activities and the prevention activities and I think this highlights that and his reorganization does it.

Second, I think it highlighted the changed nature of the expectation of the private sector and the government in restoring, particularly for those assets that have significant natural impacts such as the pipelines, refineries, etc. and it increases our need for information sharing, for something simple as working to make sure the aerial photography that we take very quickly after it gets to the owners and operators who don't have access to the sites they can begin their response. We can share things that historically we did not connect the two together so I think it will have that kind of practical impact.

Mr. PLATTS. Thank you, again to each of you. We appreciate your written testimonies, your testimonies here today and each of your respective organization's work of you and your colleagues on behalf of our fellow citizens. Thank you.

We'll take again a brief 2 minute recess where we'll get our third and final panel set up and reconvene shortly.

[Recess.]

Mr. PLATTS. This hearing stands back in session. We're delighted to have on our third panel some members from the private sector to share their insights. We have Katherine Allen, chief executive officer of BITS Financial Services Roundtable; Mr. Donald Donahue, chairman, Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security; Mr. Samuel Gaer, chief information officer, New York Mercantile Exchange, chief executive officer NYMEX Europe Limited; and Mr. Steve Randich, executive vice president of operations and technology and chief information officer of NASDAQ Stock Market.

We appreciate each of you being here and we'll ask if you could stand and be sworn in and we'll take your testimony.

[Witnesses sworn.]

Mr. PLATTS. Thank you. The clerk will note that all witnesses affirmed the oath in the affirmative. We would again appreciate your written testimony. I call it my homework. When we were in school on a regular basis, and we had that homework. They're not the only ones to get it and the written testimony gave Congressman Towns and myself some great insights in preparation for this hearing. Again, we look forward to your oral testimony.

If you could try to keep it to 5 minutes each, which will enable us to get into a Q and A with you. Mr. Towns has a time crunch, having to leave shortly before 1. Ms. Allen, if you would like to begin.

STATEMENTS OF CATHERINE ALLEN, CHIEF EXECUTIVE OFFICER, BITS, THE FINANCIAL SERVICES ROUNDTABLE; DONALD DONAHUE, CHAIRMAN, FINANCIAL SERVICES SECTOR COORDINATING COUNCIL FOR CRITICAL INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY; SAMUEL GAER, CHIEF INFORMATION OFFICER, NEW YORK MERCANTILE EXCHANGE, INC., CHIEF EXECUTIVE OFFICER, NYMEX EUROPE LIMITED; AND STEVE RANDICH, EXECUTIVE VICE PRESIDENT OF OPERATIONS AND TECHNOLOGY AND CHIEF INFORMATION OFFICER, THE NASDAQ STOCK MARKET, INC.

STATEMENT OF CATHERINE ALLEN

Ms. ALLEN. Thank you, Chairman Platts and Mr. Towns for the opportunity to testify today. A full version of my testimony has been submitted for the record and is here today.

I'm Catherine Allen, CEO of BITS. BITS is a nonprofit industry consortium of the 100 largest financial institutions in the United States. We're a non-lobbying group, sort of a think tank for technology and operations for the CEOs of these 100 largest organizations. We serve the industry needs at the interface between commerce, technology and financial services. We're probably most well known for the best practices and guidelines that we create on behalf of the members for the industry and we share that much more broadly through the FSSCC, through other groups, to the smallest institutions to make sure that they are aware of the issues and address some of those issues.

BITS and Roundtable member companies direct about $40.7 trillion in managed assets, $960 billion in revenue and 2.3 million jobs. Our activities are driven by the CEOs and the CIOs or the

heads of security of these organizations. The risk managers and leaders who care for the financial services sector critical infrastructure.

We also work closely with government agencies such as the Department of Homeland Security, Treasury, the Federal Reserve, the FBI and many financial regulators, technology and trade associations and vendors in achieving what we try to do. The financial services industry has always taken significant steps to prepare for and respond to major events. In fact, the financial sector is often viewed as the poster child for what needs to happen in the critical infrastructure arena, primarily because of our focus on operational, fiduciary, financial and reputational risk.

Events in the past few years from September 11th to Katrina have escalated our efforts. While I believe our industry overall is better prepared than ever, there are significant risks that can only be addressed by working in partnership with others and that partnership is what I'll talk about mostly in my testimony.

Financial institutions weathered Hurricane Katrina well and now Hurricane Rita and responded to customer needs quickly. They also responded well during the August 2003 power outage and the terrorist attacks on September 11th.

Our sector is a favorite in terms of a target by cyber criminals as well as terrorists. Over the past 4 years the financial services sector has taken major strides to respond to the risks we face today and prepare to address future threats and vulnerabilities.

Financial institutions have business continuity plans which they constantly update, refine and test. This is a regulatory requirement and part of the risk management process that all financial institutions have embraced. As financial institutions identify risks, they work to mitigate them and BITS has made coordinating financial services industry crisis management efforts a top priority. Some examples of what we've done: There have been numerous conferences and meetings to bring together leaders and experts. We developed a crisis communicator for our CEOs and crisis management coordination and security executives to get them on the phone as quickly as possible. We've helped create and drive membership in the FS–ISAC, the Information Sharing and Analysis Center; we conducted worst case scenario exercises, we've engaged in partnerships with the telecommunications sector and key software providers such as Microsoft to address our industry's business requirements. We've compiled lessons learned from September 11th and from the August 2003 blackout and Hurricane Katrina and have shared those with the industry.

Most well known are our development of best practices and voluntary guidelines in everything from how you manage outsourcers to the alert levels at the Department of Homeland Security to the cross industry telecom business requirements. We're currently working on best practices with the energy industry, energy and power industries. We created a model for regional coalitions, ChicagoFIRST, and we developed liaisons and pilots with the telecommunications industry to develop the appropriate levels of diversity and redundancy. There is no true diversity and redundancy in the telecommunications system today and that was one of the things that is critical and on the top of our list.

Most recently in response to Hurricane Katrina and now Hurricane Rita, BITS stepped in to help in coordinating and disseminating critical information and, again, in my longer testimony, there are examples of that.

As you know, the financial institutions are heavily regulated and actively supervised by State and Federal agencies. Both have stepped up their oversight of business continuity, information security, third party service providers and critical infrastructure protection. And also the financial exchanges have added requirements in this area.

Regardless of how well financial institutions respond to regulations, we simply cannot address these problems alone. Our partners in other critical industry sectors, in particular telecommunications, energy and software, must all do their fair share. In fact, we call it conducting a "higher duty of care" because they respond to the critical infrastructures.

During the past 4 years, the FSSCC, the Financial Services Sector Coordinating Council for Critical Information Protection, has been created. BITS helped to establish that and continues to play a major role in its efforts. You'll hear more about that from Don Donahue in a few minutes. We work closely with the FSSCC under the Department of U.S. Treasury and with other departments at other government agencies.

There are specific examples of cooperative efforts that BITS funded and put together and share with the industry. First of all, with the Securities Industry Association, we put together best practices and what you do at different levels of security from the Department of Homeland Security's alert levels, what you do at the various orange, red and yellow levels, we shared those throughout the critical infrastructure industries.

Second, working with the U.S. Treasury, we funded or underwrote the costs for developing ChicagoFIRST so we would have a regional model and then could share that model with other member companies in other regions of the Nation. ChicagoFIRST was created to foster preparedness and recoverability of financial services in specific regions and again serves as the model for other regions.

As part of BITS' work to strengthen our critical infrastructure, we also focused on the need for more diverse and resilient telecommunications services. BITS engaged with the telecommunications companies, and worked very closely with the National Communications System, an excellent group, which is now under the Department of Homeland Security and worked with them to develop the BITS Guide to Business Critical Telecommunications Services. It's a resource for outlining what financial institutions need to ask of their telecommunications partners and in my role sitting on the NRIC, which is a group of telecommunications CEOs that respond to the—that advise the Federal Communications Commission, we also provided that information into those work groups so we could exchange the dialog with the telecommunications industry about best practices.

In dealing with Katrina's aftermath, you can see how important telecommunications resiliency and redundancy is.

Attached to my testimony is a comprehensive overview of the contributions that BITS has made in the last 2 years and, again, shared with the entire industry. They tend to focus around a few key elements: One, improving communications during crisis; two, enhancing the resiliency of the telecommunications infrastructure; third, enhancing the reliability of the electric grid, because telecom and financial services are all dependent on that; improving the security of software, hardware and the Internet; addressing forms of online fraud and identity theft and improving oversight of third party providers.

There are numerous lessons we can learn from September 11th and August 2003 and that is to be prepared and share information and view preparation from a strategic and holistic manner.

Last, some of the key things I think that the Federal Government can do is focus on this need for diversity and resiliency in the telecommunications infrastructure. There may be incentives such as using the telecommunications excise tax that could be used to incent telecommunication infrastructure changes, certainly to make available more satellite and alternative channels of communication; R&D dollars allocated to telecommunications resiliency is critically important, and again I commend the National Communications System under the Department of Homeland Security and make sure that maintains its critical role.

Second is the power grid must be considered among the vital critical infrastructures to make sure it works across the Nation. Here incentive dollars are needed and, as I said, BITS is working on best practices for this industry. The alternative power generation area is critically important for not just financial services, but all critical infrastructures.

Third, recognize the interdependence of all critical infrastructures. You cannot make requirements of the financial sector without realizing how dependent we are on telecom and power, and in some ways on the transportation industry. BITS has worked very closely with the chemical, the telecom, the power, energy and other critical industries to share what we're doing and to share best practices with them, but again, making sure that what's of vital importance is how this interdependency is addressed from the Government level.

Last, and I would say probably most importantly, all of us at BITS worry about a combined physical and cyber attack. We have not had that, but I will tell you that all of the Nation's data systems; the first responder systems, the hospital systems, the police systems, the financial systems, rely on pretty much one operating system. The need for us to make sure that our operating systems and software, our hardware and our networks are secure and that there are alternatives if they are not available is critically important and that's what we mean by the "higher duty of care" for providers of those services.

I've attached to my testimony a document we call "PREPARE," which are seven things that we believe the government can do with regard to cyber security issues and again they include everything from promoting the issues and educating the consumers and the industry to providing R&D dollars to strengthening law enforcement who address cyber security issues. One other issue and that's in re-

sponse, Congressman Towns, to your question about TRIA. We think it's critically important. It's a tool that provides liquidity in the property and casualty insurance markets. Thus far, it has not cost taxpayers any money, but has resulted in the placement of a significant amount of terrorism coverage. We encourage you to reauthorize TRIA and continue with that, because it's a piece of this holistic look at terrorism.

Finally, Hurricane Katrina has made poignantly clear we need to improve coordination procedures across all infrastructures and with Federal, State and local government when events occur.

On behalf of both BITS and the Financial Services Roundtable, thank you for this opportunity to testify.

[The prepared statement of Ms. Allen follows:]

STATEMENT

OF

CATHERINE A. ALLEN
CEO, BITS

BEFORE THE

UNITED STATES CONGRESS
HOUSE COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, FINANCE,
AND ACCOUNTABILITY

HEARING ON CONTINUITY OF OPERATIONS IN THE FINANCIAL SERVICES SECTOR POST A MAJOR EVENT

SEPTEMBER 26, 2005

TESTIMONY OF CATHERINE A. ALLEN
CEO, BITS

Introduction

Thank you, Chairman Platts and Representative Towns for the opportunity to submit testimony before the House Committee on Government Reform's Subcommittee of Government Management, Finance, and Accountability on the subject of continuity of operations in the financial services sector post a major event.

I am Catherine Allen, CEO of BITS, a nonprofit industry consortium of 100 of the largest financial institutions in the U.S. BITS is the non-lobbying division of 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 and Roundtable member companies provide fuel for America's economic engine, accounting directly for $40.7 trillion in managed assets, $960 billion in revenue, and 2.3 million jobs. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues, moving quickly as needs arise. BITS' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses. To achieve our mission, BITS also works with government organizations including the U.S. Department of Homeland Security (DHS), U.S. Department of the Treasury, federal financial regulators, the Federal Reserve, technology associations, and major third-party service providers.

As risk managers and leaders in caring for the financial services sector critical infrastructure, the financial services industry has always taken significant steps to prepare for and respond to major events. Events in the past few years—from 9/11 to Hurricanes Katrina and Rita—have escalated our efforts. While I believe our industry overall is better prepared than ever, there are significant risks than can only be addressed by working in partnership with others. My testimony will outline the steps that BITS and others in the financial services industry have taken in recent years and actions the government can take to support our efforts.

The financial services sector is a key part of the nation's critical infrastructure. Customer trust in the security of financial transactions is vital to the stability of the financial services sector and the strength of the nation's economy. Financial institutions weathered Hurricane Katrina, and now Hurricane Rita, well and responded to customer needs quickly. Financial institutions also responded well to the August 2003 power outage and the terrorist attacks on 9/11. We know that our sector is a favorite target of cyber criminals as well as of terrorists, as was made clear on 9/11. Over the past four years, the financial services sector has taken major strides to respond to the risks we face today while preparing to address future threats and vulnerabilities.

The financial services industry has done a great deal to strengthen business continuity planning and to coordinate prior to and during times of crisis. Financial institutions have business continuity plans which they constantly update, refine and test. This is a regulatory requirement and part of the risk management process that financial institutions have embraced based on past experience, robust expertise and changing risks.

As financial institutions identify risks, they worked to mitigate them. BITS has made coordinating financial services industry crisis management efforts a top priority. Senior executives at our member companies have dedicated countless hours to preparing for the worst. We have convened numerous conferences and meetings to bring together leaders and experts, developed emergency communication tools, strengthened our sector's Information Sharing and Analysis Center (FS/ISAC), conducted worst case scenario exercises, engaged in partnerships with the telecommunications sector and key software providers, compiled lessons learned from 9/11, the August 2003 blackout and Hurricane Katrina, developed best practices and voluntary guidelines, created a model for regional coalitions, developed liaisons and pilots with the telecommunications industry for diversity and redundancy, and combated new forms of online fraud. Additionally, BITS is now developing best practices in collaboration with the electric power industry to address resiliency and recoverability issues should there be a power failure affecting financial services.

Most recently, in response to Hurricane Katrina, and now Hurricane Rita, BITS has stepped in to assist in coordinating and disseminating critical information. BITS held conference

calls with senior business continuity planning and fraud reduction officials of member companies to discuss the impact of Hurricane Katrina on members and the financial services sector overall as well as relief efforts. BITS disseminated daily updates to members beginning on September 1, serving as a repository and conduit for timely information. BITS worked closely with the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and disseminated key information to our members from regulatory agencies, Treasury and the Department of Homeland Security. Topics included assessment of impacts from the storm, efforts to deliver adequate cash supplies, FEMA's distribution of debit cards to victims of Katrina, talking points for consumer assistance, guidance from regulatory agencies, and important contacts for additional support.

As you know, financial institutions are heavily regulated and actively supervised by state and federal agencies. At the federal level, these include the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of Currency, Office of Thrift Supervision, National Credit Union Administration, and the Securities and Exchange Commission. Both federal and state level regulators have stepped up their oversight on business continuity, information security, third party service providers, and critical infrastructure protection. The financial exchanges have also added requirements in these areas. Our industry is working consistently and diligently to comply with new regulations and ongoing examinations. In addition, BITS and other industry associations have developed and disseminated voluntary guidelines and best practices as part of a coordinated effort to strengthen all critical players in the sector.

Regardless of how well financial institutions respond to regulations, we simply cannot address these problems alone. Our partners in other critical industry sectors—particularly the telecommunications, energy and software industries—must also do their fair share to ensure the soundness of our nation's critical infrastructure.

During the past four years, the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (or FSSCC) has been created. I referred to it earlier in the context of the industry's response to Hurricane Katrina. BITS helped to

establish the FSSCC in 2002 and continues to play a major role in its efforts. Its mission is to coordinate the entire financial sector and act as a focal point for engagement with all the regulators, Treasury, the Department of Homeland Security and the Federal Reserve. The FSSCC works in concert with the Treasury Department and other government agencies to address critical infrastructure and homeland security issues. The FSSCC is chaired by the financial services sector coordinator, Don Donahue, Chief Operating Officer, Depository Trust and Clearing Corporation, who is also testifying today. The FSSCC fosters and facilitates financial services sector-wide activities and initiatives designed to improve critical infrastructure protection and homeland security, based on a close alliance and cooperation with BITS and among the other FSSCC members to achieve these ends. BITS and other FSSCC members work closely with the Federal Banking Infrastructure Information Committee (FBIIC) under the leadership of the U.S. Department of the Treasury and with the active participation of numerous government agencies responsible for the safety and soundness of the entire financial services sector.

Two other examples of cooperative efforts to assist in preparing for and successfully addressing risks associated with catastrophic events are worth noting. One is our ongoing support for the work of the Department of Homeland Security, and specifically our development, with the Securities Industry Association, of a set of considerations for actions to be taken by financial institutions and the sector at each of the DHS levels of homeland security. The second is our work with the U.S. Treasury and a range of organizations in the Chicago area to establish the organization, ChicagoFIRST. ChicagoFIRST was created to foster preparedness and recoverability of financial services in a specific region, and serves as a model for other such organizations throughout the country.

As part of BITS' work to strengthen our nation's critical infrastructure, we have focused on the need for more diverse and resilient telecommunications services. BITS engaged telecommunications companies and government agencies to help mitigate some of these risks. The *BITS Guide to Business Critical Telecommunications Services* is an excellent resource for outlining the financial services industry's requirements from telecommunications service providers, including in times of disruption and crisis. In dealing with Katrina's aftermath,

that earlier work gave us a deeper understanding of the risks we face and the remedies we need to recover.

Attached to my testimony is a comprehensive overview of contributions that BITS made in 2004 and to date in 2005 to address homeland security and critical infrastructure protection concerns (see Appendix A.) Appendix B is a brief description of our activities in response to Hurricane Katrina. Similar activities are underway in response to Hurricane Rita. These efforts support the following key elements of our strategy to protect the financial services sector and its critical infrastructure:

- Improving communications during crises;
- Enhancing the resiliency of telecommunications services;
- Enhancing the reliability of the electrical grid;
- Improving the security of software, hardware and the Internet;
- Addressing new forms of online fraud; and
- Improving oversight of third party providers.

Additional details on the efforts of the entire financial services sector are outlined in a report issued by the FSSCC. See www.fsscc.org for a copy of this report.

Key Elements for Being Prepared

There are numerous lessons we can draw from 9/11, the August 2003 blackout and most recently Hurricanes Katrina and Rita. The most important and obvious is to **be prepared**. An important part of being prepared is looking strategically and holistically at the nation's critical infrastructures and what can be done to enhance resiliency and reliability. Further, it is important that we work with other parties in the private and public sectors to address these issues sufficiently. We understand that the risks for national security and economic soundness cannot be underestimated. Neither can the importance of our working together to address them.

Diverse and resilient communication channels are essential. Diverse elements—such as cell phones, wireless email devices, landline phones, and the Internet—are required. Both diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services will be maintained. Closely related to this is the importance of having accurate and timely information about the scope and cause of major events. For example, during the August 2003 blackout, the announcement that the problem was not the result of a terrorist event alleviated public concerns and enhanced the orderly execution of business continuity processes.

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

Recognize the interdependence of all critical infrastructure sectors. Those of greatest concern to us, and relevant to the topic of this Hearing, are the interdependencies between financial services, telecommunications, and energy. We believe the government should take action to enhance the diversity and resiliency of the telecommunications infrastructure and the nation's energy grids.

Recognize the dependence of all critical infrastructures on software operating systems and the Internet. A clear understanding of the role of software operating systems and their "higher duty of care," particularly when serving the nation's critical infrastructures, needs to be explored, including ways of sharing responsibility and liability more equitably. See Appendix C for a list of steps the government can take to strengthen cyber security.

And, as Hurricane Katrina has poignantly made clear, we need to 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

On behalf of both BITS and The Financial Services Roundtable, thank you for the opportunity to testify before you today.

BITS
FINANCIAL SERVICES
ROUNDTABLE

Appendix A

PROTECTING THE CRITICAL INFRASTRUCTURE: BITS' ACCOMPLISHMENTS IN 2004 - 2005

PUBLICATIONS OF BEST PRACTICES AND GUIDELINES

Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy

- The BITS study on "Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy" outlines inefficiencies resulting from regulatory overlap within:
  - The Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA);
  - The Gramm-Leach-Bliley Act of 1999 (GLBA);
  - The Sarbanes-Oxley Act of 2002 (SOX); and
  - The proposed U.S. Inter-agency Operational Risk Supervisory Guidance on Operational Risk Advanced Measurement Approaches (AMA) for Regulatory Capital (applying the International Convergence of Capital Measurement and Capital Standards: A Revised Framework, also referred to as Basel II), July 2003.
  - The study includes specific recommendations for implementation by member institutions to increase efficiencies, and further provides recommendations for regulators to work with the financial services industry to reduce unnecessary burdens and eliminate inconsistent requirements. The study will be available in hard copy in September 2005, and will be jointly distributed by BITS and the Roundtable to key regulators as well as member institutions.

BITS Consumer Confidence Toolkit and Voluntary Guidelines

- BITS has developed a *Consumer Confidence Toolkit: Data Security and Financial Services.* This Consumer Confidence Toolkit is publicly available and provides information to support consumer confidence in the safety, soundness and security of financial services. Special attention is placed on online financial services transacted through the Internet. Data in support of the safety of online financial transactions are provided. Information about the proactive leadership of the financial services industry is included, as well as a description of the current environment and recommendations for government agencies and leadership. Tips for consumers to help protect their financial security, including in the online environment, are also provided. In addition, BITS has developed Voluntary Guidelines as recommendations to member institutions for managing information security and consumer confidence issues.

BITS Critical Success Factors for Security Awareness & Training Programs

- Under the auspices of the BITS Security and Risk Assessment Program, BITS developed a description of critical factors for establishing and maintaining a comprehensive security awareness and training program for financial institution personnel. Developing a comprehensive security awareness and training program is a regulatory requirement and an effective risk management practice.

BITS Key Considerations for Global Background Screening Practices

- BITS released the *BITS Key Considerations for Global Background Screening Practices* on June 29, 2005. This document is an outstanding tool for financial institutions and other critical infrastructure companies seeking to mitigate risks related to global outsourcing. The paper is divided into three sections:
  - Overview of the financial industry's legal and regulatory requirements;
  - Strategies for evaluating the risks and mitigating controls for outsourced environments and activities; and
  - Information to validate identity and background, listed by country.
- Each section outlines financial institutions' top considerations for global employee screening policies, programs and requirements. The paper is available on the BITS website at www.bitsinfo.org on the publications page.

Key Contractual Considerations for Developing an Exit Strategy

- Published in May, 2005, the *BITS Key Contractual Considerations for Developing an Exit Strategy* provides detailed suggestions for contracts with third party service providers, many of which provide security-related services and affect critical infrastructures.

Fraud Prevention Strategies for Consumer, Commercial and Mortgage Loan Departments

- Loan fraud is a fast-growing problem. This Members' Only guide helps financial institutions catch loan frauds as they happen and recover from related losses. Members interested in obtaining a copy may access it via the BITS site, www.bitsinfo.org, in the Members' Only area.

BITS Guide to Verification, Authentication and Financial Experience Information Technology for Online New Account Openings

- In January 2005, BITS published the *BITS Guide to Verification, Authentication and Financial Experience Information Technology for Online New Account Openings.* This Members' Only guide assists financial institutions in understanding technology to verify and authenticate online users and determine the level of risk users pose to the institution. This document was created to help financial institution fraud managers as they explore these technologies and identify those that may be appropriate for their needs. This paper focuses on technology solutions for:
  - Verification. These products screen data elements provided by a client to ensure the elements (Social Security numbers, addresses, etc.) are real.
  - Authentication. Once the data elements are verified, authentication products ensure the credentials given belong to the person providing them.

- Financial experience information. Having verified the data elements and authenticated the customer, financial experience information determines the level of risk assumed by accepting the potential customer.

BITS Guide to Business-Critical Telecommunications Services

- On November 15, 2004, BITS released the *BITS Guide to Business-Critical Telecommunications Services*. The *BITS Guide* highlights questions business continuity planners and other risk managers should ask themselves as well as an overview of key points to consider in risk assessment, due diligence, contracting, testing and monitoring processes of their telecommunications services.

Improving Business Continuity in the Financial Services Sector: A Model for Starting Regional Coalitions

- The U.S. Department of the Treasury publicly released the handbook, "Improving Business Continuity in the Financial Services Sector: A Model for Starting Regional Coalitions" on December 7, 2004. This handbook is the result of a collaborative effort, funded by Treasury and co-authored by BITS, The Boston Consulting Group and ChicagoFIRST. The handbook offers "lessons learned" and clear recommendations for replicating the success of the ChicagoFIRST model in other regions. Louis F. Rosenthal, Executive Vice President, LaSalle Bank Corporation, and Ro Kumar, First Vice President of The Options Clearing Corporation are to be commended for their leadership and vision as founding co-chairs of the coalition. Teresa Lindsey, BITS Chief of Staff, was instrumental in facilitating the development of ChicagoFIRST and in distilling the "lessons learned."

BITS Kalculator: Key Risk Management Tool for Information Security Operational Risks

- The *Kalculator* starts with a list of common information security threats and vulnerabilities and matches them with corresponding controls to mitigate those risks. Using the *Kalculator*, financial institutions score their information security risks based on the likelihood of an incident, the degree to which the organization has defended itself against the threat, and the incident's possible impact. Companies can use the results to boost their ability to assess and mitigate risks. The *Kalculator* is unique in that it brings together information security risk categories from international security standards and emerging operational risk regulatory requirements into one tool that can be easily customized.

Developing a KRI Program: Guidance for the Operational Risk Manager

- The document, *Developing a KRI Program: Guidance for the Operational Risk Manager*, helps operational risk managers establish and maintain strong KRI programs in an environment of increased operational risk regulation.

Best Practices in Patch Management for the IT Practitioner

- *BITS Best Practices in Patch Management* provides critical recommendations for an enterprise approach to managing patches. Divided into 10 sections reflecting the components of effective patch management processes, the document provides

considerations for defining roles, responsibilities and tools; developing and maintaining an inventory of IT infrastructure; developing a "standard build"; and verifying patch installation. While created for financial institutions, these recommendations may be applied to other industries.

BITS IT Service Providers Expectations Matrix

- The BITS *IT Service Provider Expectations Matrix* provides financial institutions, service providers, and audit and assessment organizations with comprehensive and consistent expectations to reduce risk. Presented in an Excel spreadsheet, it outlines financial institution expectations for the security of information and personnel, as well as policies and processes for ensuring physical security. The expectations address critical disaster recovery/business continuity issues necessary to ensure products and services are supported by and coordinated with service providers.

Strategies for Mitigating Fraud Risks Associated with the Check Clearing for the 21st Century Act

- This paper provides informed analysis of the risks and benefits associated with implementation of the Check 21Act. Strategies for mitigating risks are included as well as a matrix that describes Check 21-related risks and mitigants from the standpoint of three major parties affected by the Act: the business customer that truncates checks before deposit, the bank of first deposit, and the paying bank.

COMMENT LETTERS

Comment Letter on FDIC Study, "Putting an End to Account-Highjacking Identity Theft"

- BITS, The Financial Services Roundtable and the Identity Theft Assistance Corporation jointly submitted a comment letter, raising concerns about the proposed approach to remedies for fraud-related security risks. The study did not adequately take into account the fact that financial institutions are applying a risk-based approach for evaluating the risks, deploying controls and offering convenient solutions to their customers and recommended solutions that are complex, unwieldy, and, in some instances, will not provide the intended remedy.

Comment Letter on Department of Homeland Security (DHS) Interim Rule on Procedures for Handling Critical Infrastructure Information

- BITS and The Financial Services Roundtable submitted a comment letter to DHS on a rule to establish "uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal government through the Department of Homeland Security." The letter outlines concerns about the scope and implementation of the procedures. It states that DHS must implement robust controls to adequately protect employees and customers of financial institutions.

TESTIMONY

"The Department of Homeland Security Cybersecurity Enhancement Act of 2005" to House Committee on Homeland Security Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity

- Catherine A. Allen, BITS CEO, testified in April, 2005 on the importance of elevating the position of Cybersecurity Director at the Department of Homeland Security to an Assistant Secretary level. Her testimony included a description of the current cybersecurity landscape, and what BITS and the industry are doing to address threats. The testimony also included the BITS recommendations to the government to strengthen cybersecurity, referred to in detail and presented as the acronym PREPARE©.

"Critical Infrastructure Protection" to House Financial Services Committee

- Wilton Dolloff, executive vice president for operations and technology at Huntington Bancshares and BITS Executive Committee member, testified in September on behalf of BITS and The Financial Services Roundtable before the House Financial Services Committee. The full Committee hearing was on efforts to strengthen the nation's critical infrastructure. Dolloff emphasized that all critical infrastructure sectors need to participate in ensuring the soundness of the nation's critical infrastructure.

"Information Security—Vulnerability Management Strategies and Technology" to House Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census"

- Louis Rosenthal, LaSalle Bank Corporation, testified before Congress on June 2, 2004 on how the financial services industry is working to improve software security. The hearing, titled "Information Security – Vulnerability Management Strategies and Technology," took place before the House Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Mr. Rosenthal testified on behalf of BITS and the Roundtable. He shared BITS' data on the enormous cost of addressing software vulnerabilities, including managing patches (approaching $1 billion annual cost to the industry). Mr. Rosenthal stressed that BITS is working to improve the quality of the software financial institutions use through a number of projects. He emphasized, however, that the industry must have the support of its vendor partners and government in order to be successful. His recommendations were based on those of the April BITS/FSR software security policy statement.

SUMMITS, FORUMS AND CONFERENCES

Critical Infrastructure Protection

- John Carlson represented BITS at a July 11, 2005 invitational meeting convened by Bob Stephan, Assistant Secretary for Infrastructure Protection, Department of Homeland Security. The purpose of the meeting was for DHS to get input and recommendations from association leaders who are active in cyber security issues.

- On June 17, 2005 Dartmouth's Institute for Information Infrastructure Protection (I3P) hosted a forum on "Financial Services Challenges in the Cyber World" at New York University in New York City. BITS participated in a panel discussion along with representatives from BITS member companies and key federal government agencies. Approximately 25 government and academic leaders involved in research on cyber security and critical infrastructure issues participated in the meeting.

A Strategic Look at Authentication

- On March 8, 2005, BITS hosted a Forum entitled "A Strategic Look at Authentication" in Washington, DC. Authentication issues have emerged in a number of BITS' working groups. This strategic Forum focused on the following issues: business issues that drive the need for authentication; business challenges to implementation; public policy implications; and emerging technologies in the authentication area.

BITS Regulatory Forum

- The BITS Regulatory Forum was held on April 26, 2005 and established a dialogue among regulators and financial services firms on the impact of regulatory requirements and supervisory processes. Many of those requirements relate to critical infrastructure protection and security issues. Participants reviewed steps to be taken by all parties to increase efficiency in the regulatory and supervisory process. Senior level regulators and BITS members took part in this session, the first step in an iterative, cross-sector process. The Forum was the first public release of the study, developed on BITS' behalf by KPMG, "Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy."

SRA Protecting the Core Forum: Strategies for Securing Your Technology Infrastructure

- On October 6, 2004 BITS held a Forum, "Protecting the Core: Strategies for Securing Your Technology Infrastructure." The invitation-only event allowed member companies and invited vendors to explore how significant risks and costs resulting from insecure devices, untrusted systems, and new threats and vulnerabilities impact core operations. During the Forum, executives from the financial services industry, federal government and top technology companies shared their perspectives as speakers and panelists. Speakers included Burt Kaliski, RSA Security; Scott Charney, Microsoft; Alan Paller, SANS Institute; Ido Dubrawsky, Cisco Systems; Howard Schmidt, eBay; and Edward Amoroso, AT&T. The Forum focused on sharing best practices and identifying solutions.

BITS Critical Infrastructure Forum: Strengthening Resiliency of the Telecommunications and Energy Sectors

- The BITS Critical Infrastructure Forum, "Strengthening Resiliency of the Telecommunications and Energy Sectors," was held June 9, 2004 in Washington, DC. More than 100 participants from the financial services, telecommunications, energy, and chemical sectors attended. Don Monks, The Bank of New York Company, Inc., keynoted, discussing lessons learned from 9/11. Other speakers included Fran Dramis, CIO of BellSouth, Steve Malphrus, Staff Director of the Federal Reserve Board of

Governors, Wayne Abernathy, Treasury Assistant Secretary for Financial Institutions, and Jim Caverly, Director of the Infrastructure Coordination Division in the Information Analysis and Infrastructure Protection (IAIP) Directorate of the Department of Homeland Security.

BITS and The Financial Services Roundtable Software Security CEO Summit

- The BITS and Financial Services Roundtable Software Security CEO Summit was held February 4, 2004 in Arlington, Va. This invitation-only event allowed member CEOs and CIOs to come together with the CEOs and CIOs of the chemical, telecommunications, and electric industries to discuss how risks and costs resulting from software vulnerabilities are affecting their institutions, and to develop solutions. Senior executives from the financial services industry, federal government and top software companies shared their perspectives as speakers and panelists. Taken from the industry's perspective as leading purchasers of software products, the Summit focused on identifying solutions for improving software security. Eighty participants representing senior leadership from the financial services industry, software providers, other business sectors and government discussed issues and costs related to software security and patch management—and a plan for action to address them. As follow-up to the Summit, BITS Chairman Jim Rohr, The PNC Financial Services Group, distributed a *Software Security Toolkit* to all BITS members and Summit participants.

BITS/American Banker Financial Services Outsourcing Conference

- The Fourth Annual BITS/American Banker Outsourcing Conference, will take place on November 7-8, 2005 at the Renaissance in Washington D.C. This year's agenda will follow four key themes:
  - Governance: Best practices of financial institutions and service providers.
  - Compliance: Strategies for negotiating the current landscape and requirements for privacy and security.
  - Risk Management: Strategies, controls and processes to coordinate risk management across the enterprise.
  - Change: Practical guidance for managing today's dynamic relationships.

- The Third Annual BITS/American Banker Outsourcing Conference, "Managing Risk in a Global Economy," was held on November 8 and 9, 2004 in Washington, DC. Over 150 participants representing financial institutions, regulators and service providers attended. The conference focused on four key themes:
  - Legislative and Regulatory: Strategies for negotiating the current landscape and requirements
  - Privacy and Security: Establishing and maintaining controls and requirements
  - Governance: Creating enterprise-wide accountability and strategies to effectively and efficiently manage your relationships
  - Risks and Opportunities: Identifying best (and worst) practices

Fighting Identity Theft: Outsmarting the Crooks (Joint with U.S. Treasury)

- The Treasury and BITS jointly held a Forum for consumers, "Fighting Identity Theft: Outsmarting the Crooks" on May 26, 2004 in Kansas City, Mo. The event was co-hosted by Wayne Abernathy, Treasury Assistant Secretary for Financial Institutions, and Catherine Allen, BITS CEO. Catherine outlined the financial services industry's efforts to prevent identity theft and assist victims, including the industry's Identity Theft Assistance Center, co-founded by BITS, The Financial Services Roundtable, and 50 founding member financial institutions. She also moderated a panel on innovative technologies the industry is developing to fight identity theft. Abernathy spoke about the tools available to consumers through the Fair and Accurate Credit Transactions (FACT) Act and moderated a panel discussion of the ways financial institutions are helping consumers to fight identity theft.

POLICY DEVELOPMENT

NOTE: BITS serves as a source of fact-based information in the development of policy positions. Following are recent examples, resulting either in a formal position from both BITS and The Financial Services Roundtable, or indirectly, through participation in national-level councils, working groups and task forces. Other examples of BITS' role in policy development are listed above in the categories of Comment Letters and Testimony.

- Joint BITS and Financial Services Roundtable Policy on Authentication Mandates
- Joint BITS and Financial Services Roundtable Policy on Spyware
- Joint BITS and Financial Services Roundtable Policy on Software Security
- Joint BITS and Financial Services Roundtable Policy on Internet Fraud and Phishing
- Support for President's National Infrastructure Advisory Council (NIAC)
- Participation in National Security Telecommunications Advisory Council (NSTAC) Financial Services Task Report
- Participation in Network Reliability and Interoperability Council (NRIC) VII
- Participation in Congressman Adam Putnam's Corporate Information Security Working Group (CISWG)
- Participation in the National Cyber Security Partnership

PILOTS AND PROJECTS

BITS Phishing Prevention and Investigation Network

- BITS is responding to "phishing" through its Fraud Reduction Program. Phishing is the practice of luring consumers to provide bank account and other personal information to fraudsters through bogus email messages. In response to these and other online scams, BITS created a Phishing Prevention and Investigation Network. The BITS Phishing Prevention and Investigation Network has three primary purposes. First, the Network helps financial institutions shut down online scams. Second, it helps increase arrests and investigations of scam perpetrators by providing trend data. Law enforcement agencies can use the data to build cases and stop scamming operations. Finally, the BITS

Network facilitates communication among fraud specialists at financial institutions, law enforcement agencies and service providers, resulting in a "united front" for combating online scams. Financial institutions can also use the BITS Network to share information about online scams. Through its searchable database, fraud professionals at BITS member institutions learn from other institutions' phishing incidents and responses. The database provides quick access to contacts at law enforcement agencies, foreign governmental agencies, and ISP administrators. Founded under the auspices of the BITS EScams Subcommittee of the BITS Internet Fraud Working Group, the Network is hosted by the Financial Services Information Sharing and Analysis Center (FS/ISAC). Resources to develop the Network were contributed by Microsoft Corporation and RDA Corporation.

ChicagoFIRST

- With the encouragement of the US Treasury and support from BITS, Chicago's premier financial services institutions formed ChicagoFIRST in July 2003 as an industry coalition that addresses homeland security issues requiring a common response by Chicago's financial services sector. This initiative was prompted by a consensus that existing activities at the regional level did not adequately address the critical infrastructure protection concerns of Chicago's financial institutions. The mission of ChicagoFIRST is:
  - To increase the resilience of the Chicago financial services industry in the event of a regional disaster in collaboration with the city, state and federal agencies, including to:
    - protect the lives of the thousands of people that work in the industry;
    - protect the financial assets that have been entrusted for safe keeping and investment;
    - work directly with city and state authorities on emergency coordination and evacuation; and
    - implement the primary objectives in a rapid manner.

  The "lessons learned" from ChicagoFIRST, as reported above and funded by the U.S. Treasury, were published in December 2004, with the hope that additional coalitions will successfully establish similar organizations to strengthen critical infrastructures at a regional level. The Treasury supports the concept of regional coalitions of financial services firms and will work with interested parties to facilitate their formation. For more information, please contact the Office of Critical Infrastructure Protection and Compliance Policy at (202) 622-2602.

Facilitation of Alliance for Telecommunications Industry Solutions (ATIS) Diversity Assurance Pilots

- BITS is working closely with the Alliance for Telecommunications Industry Solutions (ATIS) CIO Council on diversity-assurance pilots. (ATIS is a US-based body that works to develop and promote technical and operations standards for the communications and related IT industry worldwide.) The primary goals of the pilots are to:
  - Assess the basic requirements for an effective diversity-assurance service that meets customer needs and regulatory requirements;
  - Determine the scalability and viability of a manual process patterned after the service provided to the FAA;
  - Identify the best and most effective practices for assuring diversity in a manual mode; and define the requirements for a possible mechanized process.

Identity Theft Assistance Center (ITAC)

- The Identity Theft Assistance Center (ITAC) was initiated as a one-year pilot program intended to help victims of identity theft by streamlining the recovery process and by enabling law enforcement to identify and prosecute perpetrators of this crime. The ITAC is now officially up and running as the pilot was a success. As of August 2005, more than 2500 victims of identity theft had received assistance from the ITAC. ITAC is an initiative of The Financial Services Roundtable and BITS, which represent 100 of the largest integrated financial services companies. The ITAC's services are free-of-charge to customers and made available based on referrals to the ITAC by one of the ITAC's Members. For additional information, go to www.identitytheftassistance.org.

BITS Product Certification Program (BPCP)

- The BPCP provides product testing by unbiased and professional facilities against baseline security criteria established by the financial services industry. A product certification, the *BITS Tested Mark*, is awarded to those products that meet the defined criteria. An option is available for technology providers to meet the product certification requirements via the internationally recognized Common Criteria certification schema. BITS has initiated discussions with DHS to support efforts to enhance product certification programs, including the Common Criteria program run by the National Security Agency and National Institutes of Technology and Standards. DHS has expressed support for broad-based, not sector specific, certification programs. Moreover, DHS wants "buy in" from the broader user community. Consequently, BITS has been in discussions with The Business Roundtable, NIST, and the Cyber Security Industry Alliance (CSIA) to develop a joint proposal.

Joint Work Plans with Major Software Providers

- BITS' efforts to improve the quality of software security have three overarching objectives. BITS wants vendors to provide a higher duty of care when selling to the financial industry and other critical infrastructure companies; ensure products comply with security guidelines before releasing products; and make the patch-management process more secure and efficient and less costly for organizations. To meet these objectives, BITS is urging vendors to comply with business requirements. Under the requirements, software vendors would use security criteria, like the BITS software security criteria and the Common Criteria, in developing software products to ensure products meet minimum security standards. Companies would then test the products for security and conduct thorough code reviews prior to releasing them. To facilitate achievement of these objectives, BITS has implemented a joint work plan with one major software provider and is developing joint work plans with others.

SURVEYS AND RESEARCH

Cybersecurity R&D Priorities.

- The results of a 2005 BITS survey on cybersecurity research and development are being used to advise the federal government (Congress, Treasury, the Department of Homeland Security) on its R&D priorities. The BITS survey coincides with the

publication of a Cyber Security Industry Alliance (CSIA) paper urging the federal government to play a larger role in coordinating cyber security R&D funding. The CSIA paper notes that while the private sector contributes the majority of funds for R&D on cyber security, most of this money is for short-term solutions to existing problems. The CSIA and BITS are recommending the federal government organize long-term cyber security research to address problems before they emerge.

FOR ADDITIONAL INFORMATION, CONTACT:

Catherine A. Allen, CEO
John Carlson, Senior Director
BITS
1001 Pennsylvania Avenue NW
Suite 500 South
Washington DC 20004
(202) 289-4322
cathy@fsround.org
john@fsround.org
www.bitsinfo.org

ABOUT BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. For more information, go to www.bitsinfo.org.

Appendix B

BITS Hurricane Katrina Response (as of September 12, 2005)

Provided Daily Updates to Members. BITS disseminated daily updates beginning on September 1 to the BITS Advisory Council, BITS Crisis Management Coordination Key Contacts and Working Group, BITS Fraud Reduction Steering Committee, and Financial Services Roundtable staff. Daily updates included key information from regulatory agencies, Treasury and the Department of Homeland Security on impact assessments on infrastructure (e.g., telecom, power), efforts to deliver adequate cash supplies, distribution of debit cards by FEMA and the Red Cross to victims of Katrina, talking points for consumer assistance, and important contacts for additional support and to request mobile ATMs and satellite phones.

Hosted BITS Working Group Calls and Assisted Members. BITS held several conference calls (September 2 and 6) with senior business continuity planning and fraud reduction officials of member companies to discuss the impact of Hurricane Katrina on members and the financial services sector overall as well as relief efforts. BITS also participated in other calls by SIA and DHS to gather and serve as a repository of financial sector information.

- BITS Fraud Reduction Steering Committee (FRSC) calls focused on potential fraud and risk mitigation strategies. The FRSC asked BITS to act as a repository of information to help identify and socialize fraud trends and events as they happen.
- BITS acted as primary point of contact for Roundtable members' questions and requests for more information from DHS, Treasury and Regulators. For example, BITS assisted in finding information on where FEMA is transporting large numbers of Katrina evacuees (so that member can be better prepared) and information on which parts of the storm's disaster areas residents have been ordered to evacuate.

Coordinated with FSSCC. BITS staff maintained daily contact with Don Donahue, sector coordinator for the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). BITS provided input to a press release issued by the FSSCC on September 6. The press release outlined the sector's efforts to respond to the crisis. It provided a brief overview of the progress of the financial services sector response to the needs of customers and victims affected by Hurricane Katrina, including:

- Customers of financial institutions located in the affected areas can remain confident that our members and the sector are working constantly to ensure the continued security of their financial assets.
- Deposit insurance (thru the FDIC and NCUA) is in full force.
- Financial institutions activated business continuity plans and some institutions were operating out of their back-up sites.
- National systems for processing of payments and security settlement transactions were unaffected by the hurricane and were operating normally.
- ACH credits for Social Security payments to residents in the affected areas were generally received by the processing financial institutions.

Assisted Roundtable and Members. BITS joined The Financial Services Roundtable's Government Affairs staff in a briefing for the House Financial Services Committee on Wednesday, September 7. BITS prepared a written statement on efforts, however, the committee adjourned before BITS and other associations could speak. BITS assisted Roundtable colleagues in collecting and disseminating information regarding Roundtable members' charitable donations and relief efforts.

BITS
FINANCIAL SERVICES
ROUNDTABLE

Appendix C

PREPARE

The federal government can play an important role in protecting the nation's IT assets. The following are seven key elements that the U.S. government should support to secure information technology. These elements form the acronym, PREPARE©.

Promote. Government can play an important role in promoting the importance of secure information technology. Also, government should do more to facilitate collaboration among critical infrastructure sectors and government. Some sectors, such as financial services, are heavily regulated and supervised to ensure that customer information is protected and that financial institutions operate in a safe and sound manner. Examples of actions the government can take include:

- Government should lead by example by ensuring that the issue of cyber security receives adequate attention in the Department of Homeland Security. Today, cyber security is handled at a level far below where most corporations handle these issues. Congress could create a more senior-level policy level position within DHS to address cyber security issues and concerns and ensure that adequate funding is provided.
- Strengthen information sharing coordination mechanisms, such as the Information Sharing and Analysis Centers (ISACs), by ensuring adequate funding is made available to Federal agencies sponsoring such organizations. Information sharing and trend analysis within a sector is essential to protecting information security and responding to events. Information sharing among sectors is equally important as cyber threats sometimes reach some sectors before others.
- Create an emergency communication and reconstitution system in the event of a major cyber attack or disruption of information networks. Such an attack or disruption could potentially cripple many of the primary communication channels. To allow maximum efficiency of information dissemination to key individuals in such an event, a thorough and systematic plan should be in place. The financial services industry has developed such a plan for industry-specific events in the BITS/FSR Crisis Communicator. Other organizations have developed similar communication mechanisms. These emergency communications programs should be examined as potential models for a national cyber security emergency communication system.
- Reform of the Common Criteria/National Information Assurance Partnership (NIAP). The current software certification process is costly, inefficient, used on a

limited basis by the Federal government, and virtually unknown to the private sector. NIAP should be reformed so that it is more cost effective for vendors to seek certification while ensuring consistent Federal procurement practices and expanded commercial adoption of NIAP-certified products. The BITS Product Certification Program may well be able to serve as a model.

Responsibility. Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products. Examples of actions the government can take include:

- Provide tax or other incentives for achieving higher levels of Common Criteria certification. Incremented incentives would help to compensate companies for the time and cost of certification. This should encourage certification and increase the overall security of hardware and software.
- Provide tax or other incentives for certification of revised or updated versions of previously certified software. Under Common Criteria, certification of updated versions is costly and time consuming. Incentives are necessary to ensure that all software is tested for security
- Require software providers to immediately notify ISACs of newly discovered cyber threats and to provide updated information on such threats until an effective patch is provided. It is vital that critical infrastructure companies receive immediate notice of serious vulnerabilities.
- Establish requirements that improve the patch-management process to make it more secure and efficient and less costly to organizations.

Educate. Communicate to all users of information technology the importance of safe practices. Public confidence in e-commerce and e-government is threatened by malicious code vulnerabilities, online fraud, phishing, spam, spyware, etc. Ensuring that users (home users, businesses of all sizes, and government) are aware of the risks and take appropriate precautions is an important role for government and the private sector. Examples of actions the government can take include:

- Fund joint FTC/DHS consumer cyber security awareness campaign. The FTC should focus its efforts on building consumer awareness, and DHS should coordinate more detailed technical education regarding specific serious threats. In addition, government employees should be trained in proper cyber safety measures.
- Train government employees on proper cyber security measures.
- Educate corporate executives and officers regarding their duties under Sarbanes-Oxley, GLBA, and HIPAA as they relate to cyber security.

Procure. Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the IT industry to deliver and implement more secure systems. Examples of actions the government can take include:

- Require high levels of cyber security in software purchased by the government through procurement procedures. Extend such requirements to software used by government contractors, subcontractors, and suppliers.

- Provide NIST with adequate resources to develop minimum cyber security requirements for government procurement. NIST should include software developers and other stakeholders in the standard-creation process.

Analyze. Government should collect information and analyze the costs and impact of information security risks, vulnerabilities and threats and provide this analysis to policy makers. Examples of actions the government can take include:

- Assign to the Commerce Department or another appropriate agency the responsibility of tracking and reporting such costs and their impact on the economy. Measuring and making these costs transparent will aid law makers and regulators as they assign resources to cyber security programs.

Research. Government can play an important role in funding R&D in the development of more secure software development practices, testing and certification programs. In addition, training future generations of programmers, technicians and business leaders that understand and manage information security can be accomplished by establishing university and educational/certification programs. Government can help by facilitating collaboration with the users and suppliers of IT to develop standards for safe practices. Examples of actions the government can take include:

- Enhance DHS, NSF, and DARPA cyber security R&D funding.
- Carefully manage long- and short-term R&D to avoid duplication.
- Establish a mechanism to share educational training and curricula.

Enforce. Law enforcement must do more to enforce, investigate and prosecute cyber crimes here and abroad. Examples of actions the government can take include:

- Ratify the Council of Europe's Convention on Cybercrime.
- Enhance criminal penalties for cyber crimes.
- Make cyber crimes and identity theft enforcement a priority among law enforcement agencies.
- Encourage better coordination among law enforcement agencies in order to detect trends.

For additional information, contact:
Catherine A. Allen, CEO, BITS
Or
John Carlson, Senior Director, BITS
1001 Pennsylvania Avenue NW
Suite 500 South
Washington DC 20004
(202) 289-4322
cathy@fsround.org
john@fsround.org
wwwbitsinfo.org

Mr. PLATTS. Thank you, Ms. Allen. Mr. Donahue.

STATEMENT OF DONALD DONAHUE

Mr. DONAHUE. Chairman Platts, Ranking Member Towns, thank you for inviting me today. As you know, I currently serve as chairman of the Financial Services Secretary for Coordinating Council for Critical Infrastructure Protection and Homeland Security. Which you've already heard referred to as the FSSCC, an industry group dedicated to infrastructure protection efforts. I'm also chief information officer of the Depository Trust and Clearing Corp., one of the key industry infrastructures. Through its subsidiaries, DTTC processes most U.S. trades and a broad range of financial assets, for example, last year clearing and settling 1.1 quadrillion worth of financial transactions.

FBIIC was established by the sector in 2002. It currently has 33 members consisting of many of the key industry infrastructure organizations and trading markets and a broad array of industry trade associations representing an estimated 8,000 financial institutions. The FBIIC's mission statement states that it seeks to foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve critical infrastructure protection and Homeland Security. As I will discuss later, FSSCC has very real achievements in realizing this mission.

The foundation for FBIIC's achievements is a very effective partnership with our key Federal counterparts, most particularly our strong relationship with the Department of the Treasury. Our sector-specific agency under HSPD7, has been the essential foundation for many of the sector's accomplishments in promoting infrastructure protection. The leadership of the Treasury's Office of Critical Infrastructure Protection has been invaluable in these achievements. The sector also is forming an effective relationship with the Department of Homeland Security and will continue to work with DHS in coordination with the Treasury to support its infrastructure initiatives. We also have effectively worked with the financial regulatory bodies to help them formulate and implement appropriate regulatory standards in this area.

Earlier this year FSSCC published its report, "Protecting the U.S. Critical Financial Infrastructure: 2004 In Review," a copy of which was made available to your staff. Let me mention a few examples of the sector's accomplishments identified in that report.

Prominent among them is promoting broad participation, broader participation in the Financial Services Information Sharing and Analysis Center, the sector's mechanism for sharing critical information about physical and cyber security threats and vulnerability. The FS ISAC reports it now has 1,749 participants plus an expanded reach through the sector's trade associations representing nearly 10,000 firms.

Sector members have implemented several capabilities promoting more effective disaster recovery coordination in regions critical to financial services. You've already heard much about the example of ChicagoFIRST. Other regions have implemented similar coalitions and FBIIC and its members are working with Treasury to promote this model in other areas across the country.

Third, coordinating the creation of a unified structure of emergency calls so that calls can be timed in a way to reduce conflicts and feed information into decisionmaking processes in an effective way. One of the key learnings that came out of the August 2003 blackout experience. These are a few examples of the accomplishments that the report highlights. FBIIC's own initiatives build on the very strong record of the sector generally in responding to these new infrastructure protection challenges.

My own company, DTCC, for example, has put in place a far more resilient infrastructure supporting the financial markets, even though we continued to operate without interruption during the week of September 11th, completing more than $1.8 trillion worth of financial transactions that week. The industry's other core clearing and settlement organizations and the trading markets have implemented a variety of steps since September 11th to reinforce the resilience of their operations. In addition, key trading markets have thought through reciprocal arrangements to trade in other markets' financial instruments in an extreme emergency. Sector trade associations, the Financial Services Roundtable, BITS, the Futures Industry Association, the Securities Industry Association and many others have organized their members' efforts to improve resilience practices and to test those improved practices. Much detail regarding these initiatives is set forth in the 2004 annual report. Thanks to these efforts, the sector is to the point where I am very confident of our ability to operate with minimal disruption even under very severe circumstances.

As successful as these programs have been, we also need to rehearse these practices to insure that they will work when needed. The sector's commitment to doing this as well has been exemplary. A notable example is the test plan for October 15th, in approximately 3 weeks, sponsored by the Futures Industry Association, the Securities Industry Association and the bond market Association. In this test more than 200 participants in the futures and securities industries will operate from their backup centers and test interaction with key markets and market infrastructures. FSSCC also is sponsoring a comparable test or considering sponsoring a comparable test on the payment systems side in 2006 and we expect to be making a decision about that reasonably soon.

The financial services industry has responded strongly to the new challenge of business continuity in the post September 11th world. We have done this because of our very clear understanding that we are responsible for the financial assets of 270 million Americans and for their ability to continue to conduct their financial affairs. The people of our industry take this responsibility very seriously. This committee and the Congress can rest assured that the financial services sector is and will continue to be resilient and strongly prepared for future emergency situations.

Thank you very much.

[The prepared statement of Mr. Donahue follows:]

Sector Coordinating Council for
Protection and Homeland Security

Written Testimony of

Donald F. Donahue

Chairman

Financial Services Sector Coordinating Council for

Critical Infrastructure Protection and Homeland Security

Before the

Committee on Government Reform

Subcommittee on

Government Management, Finance and Accountability

United States House of Representatives

September 26, 2005

INTRODUCTION

Chairman Platts, Ranking Member Towns and Distinguished Members of the Subcommittee on Government Management, Finance and Accountability, thank you for inviting me to testify today about the progress made over the past four years in improving the ability of the financial services infrastructure in the United States to sustain its operations in the event of a wide-scale disaster. I am Donald F. Donahue, and I currently serve as Chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (the "FSSCC"), an industry group dedicated to infrastructure protection efforts.

I am also Chief Operating Officer of The Depository Trust & Clearing Corporation ("DTCC"), and President and COO of two of its key operating subsidiaries, The Depository Trust Company and National Securities Clearing Corporation. DTCC is the largest private post-trade financial services infrastructure in the world, and provides clearance, settlement and information services for two and half million securities issues from the United States and 100 other countries and territories, including equities, corporate and municipal bonds, government and mortgage-backed securities and over-the-counter derivatives.

BACKGROUND ON FSSCC

I should begin with an explanation of who the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security is and what role it plays in the financial services sector's infrastructure protection efforts. The FSSCC was established by the financial services sector in the Spring of 2002, in response to encouragement from the Department of the Treasury, as a means of coordinating within the sector to address infrastructure protection activities. The FSSCC's mission statement states that it seeks to

> Foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security

FSSCC currently has 33 members, consisting of many of the key industry infrastructure organizations and trading markets and a broad array of industry trade associations, representing an estimated 8,000 financial institutions; a list of these members is attached to my written testimony.

FSSCC's principal responsibility is to coordinate infrastructure protection activities across the sector. There are a number of initiatives that individual sector infrastructures and associations have launched over the past four years to support the sector's response to the challenges of this "post 9/11" world. FSSCC has sought to avoid duplicating or creating conflicts with all of that work. Instead we've sought to coordinate it – for example, to link up similar efforts to address a particular problem to generate a consolidated solution that provides greater value for the sector and the nation, to ensure

that best practices developed in one area get publicized to other parts of the sector so that all get the benefit of them, or to synchronize the crisis management actions planned across the sector so that information needed for decisions flows to decision makers and information about those decisions flows out to those needing it on a timely basis. As I will discuss later, FSSCC has very real achievements to point to on each of those examples.

OUR FEDERAL PARTNERS

It's important first to set the context for the discussion of these achievements, however, by describing the very effective partnership between the sector and its key Federal counterparts that has been the basis for them. Most particularly, the strong relationship the sector has formed in this area with the Department of the Treasury, the "sector specific agency" for Banking and Finance under Homeland Security Presidential Directive Seven, has been the essential foundation for many of the accomplishments at the sector level in promoting infrastructure protection. The leadership of the Treasury's Office of Critical Infrastructure Protection on this issue has been invaluable in a number of the industry's key achievements – particularly in the establishment and growth of the sector's revamped Information Sharing and Analysis Center, the creation of ChicagoFIRST and other sector regional coalitions to promote coordinated business recovery capabilities, dissemination through the sector of "best practice" information countering the rising number of "phishing" attacks, development of a sector agenda for research and development initiatives to promote infrastructure protection, particularly in the cybersecurity area, and other efforts.

Although Treasury, as our "sector specific agency," is our primary governmental counterpart, the sector also is forming an effective relationship with the Department of Homeland Security ("DHS"), and will continue to work with DHS – in coordination with the Treasury – to support its infrastructure protection initiatives. We also have effectively worked with the financial regulatory bodies – FSSCC's public sector counterpart, the Financial and Banking Information Infrastructure Committee, and the individual agencies – to help them to formulate and implement appropriate regulatory standards in this area.

The agencies' ***Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*** identified what sector members view as the "benchmark" for resilience, and those sector members subject to these standards are meeting the required time frames to address their implementation. (The ***Sound Practices*** paper is available on the FSSCC website at http://www.fsscc.org/reports/interagency_white_paper.pdf.)

DHS has stressed in its own publications the critical importance of a vibrant public-private sector partnership in achieving the nation's infrastructure protection objectives; we believe the public-private sector partnership that has operated so successfully in financial services is an exemplary illustration of what such partnerships can achieve.

FINANCIAL SECTOR ACCOMPLISHMENTS

Earlier this year FSSCC published its report ***Protecting the U.S. Critical Financial Infrastructure: 2004 in Review***; copies of the report have been made available to the Committee. (The report is also available on the FSSCC website at http://www.fsscc.org/annual.pdf.) Let me mention a few examples of the financial services sector's accomplishments identified in that report:

- First and foremost, the sector has been very successful in promoting broader participation in the Financial Services Information Sharing and Analysis Center (the FS/ISAC), the sector's mechanism, founded in 1999, for sharing critical information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical financial infrastructure. The FS/ISAC, which had 66 members prior to the launch of the revamped FS/ISAC late in 2003, reports that it now has 1,749 participants, plus an expanded reach through the sector's trade associations approaching nearly 10,000 firms. FSSCC and its members have worked hard to support growth in the ISAC's participation. Several FSSCC member associations, for example, have joined the ISAC and redistributed its notifications to their members. Others have communicated repeatedly with their members to promote ISAC participation. The American Bankers Association has directly enrolled members to receive ISAC alerts (about 700, in ABA's case), as has my own organization.

- Sector members have implemented several capabilities promoting more effective disaster recovery coordination in regions critical to financial services. For example, ChicagoFIRST, a regional coalition formed by financial services institutions in the Chicago area, has dramatically improved coordination within the financial sector and between the sector and State and local governmental authorities in Illinois to respond much more effectively in crisis situations. ChicagoFIRST has sponsored several very successful disaster recovery simulation exercises, and also tested its capabilities in a real situation when a Chicago bank experienced a serious fire in its headquarters building. Other regions have implemented similar coalitions (for example, in New England and Minnesota), and FSSCC and its members are working with the Department of the Treasury to promote this model in other areas of the country.

- Several FSSCC member associations and organizations have put into effect standing structures of "crisis management" conference calls that would permit association members to coordinate among themselves in the event of a disaster – these types of calls were very effective in addressing problems in the sector's payment and settlement systems during the days following September 11th. The experience of the blackout in the Northeast in August 2003, however, made clear that the numbers of crisis management calls and the lack of any coordination across these different call structures could impair their effectiveness and impede information flows needed to make timely decisions about how to respond to the emergency. During the ensuing months FSSCC worked with key member

associations to coordinate the creation of a unified structure of emergency calls so that calls were timed in a way to reduce conflicts and feed information into decision-making processes in an effective way.

These are a few examples of the accomplishments the report highlights.

As the report makes clear, the Council's own initiatives seek to build upon and leverage the very strong record of efforts by the financial services industry generally to respond to the infrastructure protection challenges of this "post 9/11" environment.

- My own company – DTCC – for example, has aggressively moved over the past several years to put in place a far more resilient infrastructure supporting our functions in the financial markets, even though we continued to operate without interruption during September 11th and the following days, completing more than $1.8 trillion worth of financial transactions that week.

- The industry's other "core clearing and settlement organizations" – handling payment and securities and derivative settlement transactions – have implemented a variety of steps since September 11th to reinforce the resilience of their operations, ranging from the same type of duplicated and regionally dispersed operations my company has implemented to reciprocal backup arrangements between organizations and similar steps. The trading markets have similarly implemented reinforced business continuity and infrastructure protection programs. For example, a quick walk through the intersection of Wall and Broad Streets in downtown Manhattan will give you a very graphic illustration of the New York Stock Exchange's extensive efforts to protect its physical facilities. In addition, key trading markets have thought through reciprocal arrangements permitting one market to trade another market's financial instruments in an extreme situation where the latter market was completely unable to operate.

  These efforts have been a major focus of attention for all of these organizations over the past years, and have improved what was already a very high level of resilience in the financial service industry's infrastructure. The sector is to the point where I am very confident of our ability to operate with minimal disruption even under very severe circumstances. Notwithstanding these very substantial successes, we all remain strongly committed to this effort. To this end, the FSSCC convened this past Friday a working group of all of these core organizations to discuss how we can collaborate to generate further improvements and to benefit from our experiences so that we can do so in the most cost-effective way possible.

- In parallel to the work of the core industry market and infrastructure organizations over the past several years, individual firms and banks have implemented similar improvements to their own capabilities to withstand the consequences of an emergency situation. Sector trade associations – the Financial Services Roundtable/BITS, the Futures Industry Association, the Securities Industry

Association, and many others – have helped to organize their members' efforts, both to improve resilience practices and to test those improved practices; much detail regarding all of these initiatives is set forth in the Appendix to FSSCC's report for 2004. There has been considerable sharing of "best practices" as those have evolved, with several of these organizations publishing guides or standard practice manuals to educate their members on "state of the art" business continuity practices.

- There has been a particular focus on the issue of telecommunications resilience – the weak spot revealed on September 11th that necessitated the four-day closure of the equities markets. Industry participants have developed and shared a wealth of information on how the financial services industry can improve the resilience of its telecommunications connectivity – for example, the ***Guide to Business-Critical Telecommunications Services*** published by the Financial Services Roundtable/BITS, the ***Report of the Assuring Telecommunications Continuity Task Force*** of the Payments Risk Committee of the Federal Reserve Bank of New York, and the ***Financial Services Task Force Report*** to the President's National Security Telecommunications Advisory Committee. All of these have been made available on FSSCC's website, along with FSSCC's own summary and guidance to financial institutions on this issue (a copy of which is attached to my written testimony).

- Similar efforts are under way to identify and publicize industry "best practices" on ensuring power resilience, employee safety and security issues, and other topics. These efforts illustrate both the financial services industry's strong response to the lessons of September 11th, and the positive role the FSSCC has played in coordinating activities across the sector to maximize the benefit the financial services industry and its customers, the people of the United States, derive from these efforts.

FINANCIAL SECTOR TESTING EFFORTS

As successful as the industry has been in developing and implementing improved business continuity practices, it is, of course, essential that we test those practices to ensure that they will work when needed. Again, I believe the financial industry's commitment to testing these new procedures has been exemplary. My own organization has required its key members to test annually since 2003, and other industry infrastructure organizations have followed similar approaches. Industry associations have also worked with their members to conduct testing programs over the past several years.

A particularly notable example of this is the test planned for October 15th that is concurrently sponsored by the Futures Industry Association, the Securities Industry Association and The Bond Market Association. In this test, participants in the futures and securities industries will operate from their backup centers and test interactions with key markets and market infrastructures to ensure that they are able to connect to those

infrastructures and submit and receive transactions with them. More than 200 of the major financial institutions are expected to participate in this test, providing broad coverage of market activity – the participants for the futures industry, for example, represent more than 95% of all activity with the U.S. futures markets. FSSCC is sponsoring a discussion among its members about a comparable test on the payment systems side in 2006, building on the ongoing programs each payment system has for testing with its members to conduct a coordinated test across the whole payment system infrastructure.

CONCLUSION

The financial services industry has responded strongly and effectively to the new challenges of business continuity in the "post 9/11" world. We have done this because of our very clear understanding that we are responsible for the financial assets of 270 million Americans and for their ability to continue to conduct their financial affairs. The people of our industry take this responsibility very seriously. This Committee and the Congress can rest assured that the financial services sector is and will continue to be resilient and strongly prepared for future emergency situations.

Thank you again for the opportunity to testify at this important hearing about financial sector resilience. I would be pleased to answer any questions you may have.

Membership (as of September 15, 2005)

- America's Community Bankers
- American Bankers Association
- American Council of Life Insurers
- American Insurance Association
- American Society for Industrial Security (ASIS) International
- BAI
- BITS/The Financial Services Roundtable
- ChicagoFIRST, LLC
- Chicago Mercantile Exchange
- CLS Group
- Consumer Bankers Association
- Credit Union National Association
- The Depository Trust & Clearing Corporation (DTCC)
- Fannie Mae
- Financial Information Forum
- Financial Services Information Sharing and Analysis Center (FS-ISAC), LLC
- Financial Services Technology Consortium
- Futures Industry Association
- Independent Community Bankers of America
- Investment Company Institute
- Managed Funds Association
- The NASDAQ Stock Market, Inc.
- National Association of Federal Credit Unions
- National Association of Securities Dealers (NASD)
- NACHA — The Electronic Payments Association
- New York Board of Trade (NYBOT)
- The Clearing House
- Securities Industry Association (SIA)
- Securities Industry Automation Corporation (SIAC)
- The Bond Market Association
- The Options Clearing Corporation
- VISA USA Inc

Statement on Telecommunications Resiliency

At its meeting on September 14, 2004, the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security approved this Statement on Telecommunications Resiliency for distribution to members of the financial services sector in the United States.

Assuring the resiliency of the financial services sector of the United States is a critical objective of national homeland security efforts. Ensuring that the financial assets of the citizens of the United States and their ability to conduct financial transactions are secure helps to preserve public trust and confidence in the national economy and the national financial system. Financial services firms can do and are doing much to provide this assurance through upgraded physical and cyber security procedures, strengthened backup capabilities and other steps to improve their resilience.

Financial services firms, however, are also dependent on services from other economic sectors in the United States – most notably the telecommunications sector. Without resilient telecommunications capabilities, many financial services firms would be unable to conduct more than minimal operations. The infrastructure supporting financial services – the markets and payment and settlement systems – would grind to a halt. Financial services firms must therefore be able to rely on fully resilient telecommunications capabilities from their telecommunications services providers – assuring telecommunications resiliency is essential to meeting various regulatory requirements and guidance for the critical services provided by the financial services sector. This represents a shared responsibility, however – financial services firms must both work with their providers to ensure resiliency and also take internal steps in their own organizations to achieve these protections.

In recent months several committees have published reports with recommendations on practices and procedures financial services firms can use to improve the resilience of their telecommunications services. The recommendations in these reports are of broad interest to financial services firms, though individual recommendations may have different implications for different firms, depending on their size, mix of business, etc. The FSSCC urges all financial firms to familiarize themselves with these reports and their recommendations, and consider how to implement appropriate recommendations from these reports in their own organizations.

Copies of these relevant documents are available on the FSSCC Website at the indicated URLs. These documents are:

- A Notice from the Federal Reserve Board regarding "Sponsorship for Priority Telecommunications Services of Organizations That Are Important to National

Security/Emergency Preparedness" (the "Federal Reserve Notice"), issued December 9, 2002 available at http://www.fsscc.org/reports/Fed_Notice.pdf

- The Financial Services Task Force Report of the President's National Security Telecommunications Advisory Committee (the "NSTAC Report"), issued April 2004, available at http://www.fsscc.org/reports/NSTAC.pdf

- The Report of the Telecommunications Task Force of the Payments Risk Committee of the Federal Reserve Bank of New York (the "PRC Report"), issued September 2004 available at http://www.fsscc.org/reports/PRC_Telecom_Study.pdf

In addition, the FSSCC is aware that BITS is preparing another document, the *BITS Key Considerations for Achieving Diverse and Resilient Telecommunications Services,* which is intended to provide financial institutions with recommended practices for managing risks associated with telecommunications services. The FSSCC anticipates distributing this document to financial services firms shortly after it is published later this year.

While the FSSCC believes that anyone in the financial services sector who has responsibility for business continuity and/or for telecommunications support must carefully review the contents of these reports, certain sections of the documents are particularly important:

1. Efforts to improve overall telecommunications resiliency are being taken at the national level by regulatory authorities and industry organizations, including the FSSCC. It is likely that these national efforts will focus on those telecommunications circuits identified as National Security/Emergency Preparedness (NS/EP) circuits under programs such as the Telecommunications Service Priority (TSP) program. As noted in the NSTAC Report (at page 21), "an institution's restoration and recovery plan should include the TSP program as a key component," where possible. This program, and how to qualify circuits as NS/EP circuits under this program, is described in the Federal Reserve Notice.

2. Telecommunications resiliency depends on actions taken by telecommunications services providers and on actions taken by individual financial services firms. The resilience of services provided by a telecommunications services provider is often a matter of contract between the provider and its customer, and a clear understanding between the contracting parties is essential to ensuring that the contract provides the level of resilience desired. The discussion of "diversity, redundancy and recoverability" in the NSTAC Report at pages 2-5 makes clear that telecommunications services providers and financial services firms often use these terms in different ways, creating difficulties in reaching agreement on the level and type of resilience being contracted for. It is particularly important for financial services firms to have a full understanding of the "means of achieving diversity" of connectivity outlined in the NSTAC Report on page 3 and in Appendix B to the NSTAC Report, and to use this information in their discussions on this issue with

their telecommunications services providers. Section 4.1.3 of the NSTAC Report also contains a discussion of this contracting issue.

3. Achieving telecommunications resiliency also is the responsibility of the financial services firm with respect to those issues it can control. The PRC Report enumerates a number of suggested practices firms should consider in their own operations to achieve this end. Firms should particularly focus on the recommendations in Best Practice #1 (pages 6-7) and Best Practice #3 (page 8) of the PRC Report.

4. Achieving assured and auditable "diversity" in a set of telecommunications connections is not simply an issue at the time of installation – as telecommunications services providers manage their own operations, actions may be taken that cause a "loss of diversity" of existing circuits in ways that the contracting financial services firm may not understand. Creating procedures to monitor existing circuits to prevent or correct this inadvertent "loss of diversity" is a complex problem that will be difficult to resolve. The Alliance for Telecommunications Industry Solutions (ATIS) has inaugurated a National Diversity Assurance Initiative to identify ways to address this issue. The issue and the ATIS initiative are discussed in the NSTAC Report at pages 10-12.

The FSSCC urges all financial services firms to consider carefully the issue of telecommunications resiliency and the practices suggested in these reports.

Mr. PLATTS. Thank you, Mr. Donahue. Mr. Gaer.

STATEMENT OF SAMUEL GAER

Mr. GAER. Good afternoon. Thank you, Chairman Platts, and Representative Towns for inviting me to participate in today's hearing. The subject matter of this hearing is of an ongoing concern and engaging these issues head-on is an important tool in a set of responsible business practices for both private industry and government alike. I sincerely welcome the opportunity to express what the New York Mercantile Exchange or NYMEX has accomplished to date. The exchange is the world's largest physical commodity futures exchange and has been an example of market integrity and price transparency throughout it's 133-year history. The Exchange also plays a vital role in the commercial, civic and cultural life in New York. It provides thousands of jobs in financial services and allied industries and through its charitable foundation supports cultural and service programs in the downtown community of New York, throughout the Tri-state area where our traders and staff live, in Washington, DC, and Houston.

The business continuity planning process requires commitment from management and the ability to foresee various contingencies. Our leading role in the energy and metals markets demands we take steps to insure that our price discovery and formation mechanisms will continue to be available in the event of an emergency affecting our operations. NYMEX has a proven track record that demonstrates a dedication to insuring that we can provide our services even in the face of extreme adversity.

We are not satisfied, however, to rest on successes of past performance. As such, we continually analyze and improve our business continuity plans. The Exchange's emergency preparedness may be broken down into several distinct but integrated categories. Business continuity planning, the more narrowly focused practice of recovery planning, the education of critical staff responsible for emergency preparedness and finally the Exchange's external efforts, including coordinated industry-wide testing and provide valuable feedback to government industry agencies.

The Exchange's business is comprised of many different process groupings, each of which requires a particular expertise. These business units are each assigned a staff member who acts as a business continuity coordinator [BCC], whose responsibilities include assessing the critical processes and creating a workable recovery plan. The BCC is an individual with experience in the procedures of their specific business unit. Tactical decisions rest with the Emergency Operations Team, the OOT, which is comprised of BCC's and business continuity leaders. The BCL's role is to coordinate the Exchange's continuity and disaster recovery efforts, lead the EOT and report to the crisis management team. During an emergency, the high level strategic decisionmaking authority rests with the CMT, the Crisis Management Team, which is comprised of members of NYMEX board of directors, executive committee and critical senior executives. Their role is to assess the threat and if necessary provide an official declaration of disaster, communicate with members of the Exchange and coordinate with regulatory and industry agencies. The CMT is empowered by the board of directors

to make critical decisions necessary in any emergency recovery effort.

NYMEX's core business is commodity futures trading clearing. In order to insure the continuity of this business we have developed several alternative continuity plans. The Exchange headquarters, for instance, were designed to be as redundant as possible, including the availability of a backup generator fueled by, of all things, diesel fuel, which was critical during the September 11th terrorist attack and the blackout of August 2003.

One of the first priorities for the Exchange after recovering from September 11th was to build a completely redundant replica trading facility. This facility, which was completed in January 2003 is located outside of the city and is a reasonable commute for our staff and traders. It contains fully operational trading ring, telephone work stations and space and administrative space. More importantly, it also has the ability to disseminate price data worldwide and is a completely redundant data center, housing all critical Exchange IT systems. All of our traders and key employees have been provided with directions to the site and many of our traders have participated in a mock trading simulation actually bringing them out to the site and going through an actual trading session where they exchange trades and we ran through the clearing cycle.

In a situation where access to the trading facility in lower Manhattan or the backup site would not be immediately available, the Exchange also has two electronic trading systems, NYMEX Access and NYMEX ClearPort, both of which have 24-hour trading capability. In fact, we were the first Exchange in New York to open following September 11th. Although it was preferred that the trading would resume by open outcry, a preferred venue of trading, it was apparent that the quickest way to reopen markets would be through NYMEX access, despite the destruction of the proprietary communication circuits in the collapsed Twin Towers. The Exchange was the first New York financial market to reopen when the new system went live on Friday, September 14th. The initial energy and metals trading session was just 2 hours long, but the pent up demand for trading services resulted in then-record electronic volume of nearly 70,000 contracts. This volume was nearly eight times the average daily volume of regular 16-hour electronic trading session at that time.

In the event of an emergency, it is necessary to have a safe and secure place for teams to assemble and manage recovery efforts and coordinate services. The Exchange maintains emergency operations centers at both primary and backup sites. Should an emergency affect the primary site only, an additional temporary location has been made available through a local community relationship. Maintaining communication is the single most important aspect of any emergency recovery effort. All aspects of our emergency operations center are choreographed by multiple communication links between resources and Exchange responders. Continuity planners must envision and plan for emergencies that disable telecommunications, utilities, transportation, other infrastructure service vendors and customers.

Disaster recovery planning also specifically refers to restoring the information technologies that run our business and provide

services to staff and customers. Every critical Exchange system is duplicated and can provide services in the event the main facility or system is unavailable. Data moves across redundant fiberoptic links, linking our backup site to the primary site. In addition to wide area network or WAN created between the two hot sites the exchange maintains multiple hot links to Internet service providers. The Exchange information technology systems form the underpinnings of our ability to recover the services we provide to the marketplace in a timely fashion.

As new systems are developed and deployed at NYMEX fault tolerant distributive-active active and advance replication technologies are used to help insure we provide these services in the most adverse environments.

In September 2004, on behalf of NYMEX, I testified before the House Financial Services Committee hearing on the emergency preparedness of the financial services sector. We have since participated in the TopOff 3 exercise sponsored by the U.S. Department of Homeland Security, which was designed to test the readiness of first responders; Federal, State and local emergency managers along with key infrastructure components such as hospitals and transportation networks. The securities industry component of the TopOff 3 exercise involved the SEC, U.S. Treasury Department, exchanges and trade associations such as the Securities Industry Association, Bond Market Association and the Futures Industry Association. In addition, in October 2004 NYMEX the MIA other leading futures exchanges and clearing firms successfully completed the first industry-wide disaster recovery test. The test scope has expanded in 2005 to include market data vendors. This industry-wide disaster recovery test has become an annual event and is scheduled for October 15th.

The Exchange is among the leaders in an industry-wide initiative to standardized the protocols governing the way companies send and receive data. This will help many companies develop systems based on standardized specifications, making it easier to deploy and maintain data communications internally and externally under challenging circumstances.

Another area we have taken advantage of is sharing alliances. The Financial Services Information Sharing Analysis Center, FS-ISAC, is a source of critical information ranging from information security alerts to Homeland Security threat analysis. The New York City Office of Emergency Management is another source of information for New York-based companies. This information is critical for the constant monitoring of potential disruptive events.

NYMEX has a global presence. The Exchange's energy and metals futures markets provide benchmark pricing information that is used worldwide. NYMEX recently opened up an exchange in London and signed a joint venture agreement with the Dubai Development Investment Authority [DBIA]. The exchange must be cognizant of world events. NYMEX views continuity planning as an ongoing project that is necessary to meet critical business needs and it incorporated this planning into its day-to-day operations. Every project system or business process deployed incorporates some form of continuity planning. Risk and impact analysis, training, disaster recovering, testing and regular meetings with critical

staff create a sense of awareness throughout the company. Business continuity planning has become part of NYMEX business fabric.

We strive to learn from past experience. The September 11th terrorist attack, the 2003 blackout, our mock disaster testing and planning for the 2004 Republican National Convention, as well as the recent bombings in London which I was personally about two blocks away from, have helped us prepare for the future. This year as we were finalizing preparations for the launch of the London trading facility and during the July 7th and July 21st bombings, we activated our emergency teams as a response to that event. We are currently following important developments in the Gulf Coast region as our Nation struggles with the catastrophic damage caused by Hurricanes Katrina and Rita. As you know, there are critical delivery points for both gasoline and natural gas in that area.

Government agencies are of critical importance of preparing for and providing critical support during an emergency. The relationship the Exchange has developed with government leaders has enabled us to overcome many difficult recovery challenges. In the immediate aftermath of September 11th, we received significant assistance from the Federal, State and city governments.

The Exchange appreciates being invited to participate in these important discussions. Further efforts to improve communication between government and industry will only strengthen the ability of the Nation and financial markets to respond to the changes that lay at head. Large scale emergencies similar to those that have occurred in the past are inevitable. Continuity planning is not an individual task, but must be faced by all involved participants in the services sector.

I would like to thank the chairman and Ranking Member Towns for holding this hearing and inviting NYMEX to discuss this extremely important topic. Thank you.

[The prepared statement of Mr. Gaer follows:]

Testimony of
Samuel H. Gaer, Chief Information Officer
New York Mercantile Exchange, Inc.
Subcommittee on Government Management, Finance, and Accountability
United States House of Representatives
September 26, 2005

Good Morning. Thank you, Mr. Chairman and members of the committee for inviting me to participate in today's hearing on the preparedness of the financial services sector in a post 9/11 environment. The subject matter is of an ongoing concern and engaging these issues head-on is an important tool in a set of responsible business practices for both private industry and government alike. I sincerely welcome the opportunity to express what the New York Mercantile Exchange (NYMEX) has accomplished to date.

Introduction

The Exchange is the world's largest physical commodity futures exchange and has been an example of market integrity and price transparency throughout its 133-year history. The Exchange also plays a vital role in the commercial, civic, and cultural life of New York. It provides thousands of jobs in the financial services and allied industries, and through the Charitable Foundation supports cultural and social service programs in the downtown community of New York, throughout the tri-state area where our traders and staff live, in Washington, D.C. and Houston.

The business continuity planning process requires commitment from management and the ability to foresee various contingencies. Our leading role in the energy and metals markets demands that we take steps to ensure that our price discovery and formation mechanisms will continue to be available in the event of an emergency affecting our operations. NYMEX has a proven track record

that demonstrates its dedication to ensuring that we can provide our services even in the face of extreme adversity. We are not satisfied, however, to rest on the successes of past performance. As such, we continually analyze and improve our business continuity plans.

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

Preparedness planning cannot be accomplished without first carefully analyzing the business being protected. It is of critical importance to understand what processes make up our business. Once these are identified they must be prioritized by assessing the risks and possible impact of those risks.

Business Continuity

The Exchange's business is comprised of many different process groupings, each of which requires a particular expertise. These business units are each assigned a staff member who acts as a Business Continuity Coordinator (BCC) whose responsibilities include assessing the critical processes and creating a workable recovery plan. The BCC is an individual with experience in the procedures of their specific business unit. The duties of each continuity coordinator are in addition to the primary responsibilities of his job. Each BCC is responsible for deploying one of several plan modules. These modules are separate, but coordinated plans, which may be deployed all at once or separately as emergency requires.

Tactical decisions rest with the Emergency Operations Team (EOT), which is comprised of the BCCs and the Business Continuity Leader (BCL). The BCL's role is to coordinate the Exchange's continuity and disaster recovery efforts, lead the EOT, and report to the Crisis Management Team.

During an emergency the high-level strategic decision-making authority rests with the Crisis Management Team (CMT). The CMT is comprised of the members of the NYMEX board of directors' executive committee and critical senior executives. Their role is to assess a threat and, if necessary, provide an official declaration of a disaster, communicate with the members of the Exchange, and coordinate with industry and regulatory agencies. The crisis management team is empowered by the Board of Directors to make the critical business decisions necessary in any emergency recovery effort.

NYMEX's core business is commodity futures trading and clearing. In order to ensure the continuity of this business, we have developed several alternative continuity plans. The Exchange headquarters was designed to be as redundant as possible including the availability of a back-up generator, which was critical during the 9/11 terrorist attacks and the blackout of August 2003.

One of the first priorities for the Exchange after recovering from September 11 was to build a completely redundant replica trading facility. This facility, which was completed in January 2003, is located outside the city and is a reasonable commute for our staff and traders. It contains fully operational trading rings, telephone workstations and booths, and administrative space. It also has the ability to disseminate price data worldwide and is a completely redundant data center housing all critical Exchange IT systems. All of our traders and key employees have been provided with directions to the site and many of our traders have participated in a mock trading simulation at the site.

In a situation where access to the trading facility in lower Manhattan or the back up site would not be immediately available, the Exchange also has two electronic trading systems, NYMEX ACCESS® and NYMEX ClearPort^{sm}, both of which have 24-hour trading capability. In fact, we were the first exchange in New York to reopen following September 11. Although it was preferred that trading resume via open outcry, it was apparent that the quickest way to reopen the markets would be through NYMEX ACCESS®, despite the destruction of the proprietary communications circuits in the

collapse of the Twin Towers. An ambitious technology upgrade to shift NYMEX ACCESS® to the internet had been underway since the spring of 2001. The project was almost complete, although issues of connectivity, security, and software compatibility needed to be resolved.

Testing that was initially expected to take two weeks was accomplished in a day-and-a-half following 9/11.

The Exchange was the first New York financial market to reopen when the new system went live on Friday, September 14. The initial energy and metals trading session was just two hours long, but the pent-up demand for trading services resulted in then record electronic volume of nearly 70,000 contracts. This volume was nearly *eight* times the average daily volume of a regular 16-hour electronic trading session at that time.

Emergency Preparedness

In the event of an emergency it is necessary to have a safe and secure place for the teams to assemble and manage recovery efforts and coordinate resources. The Exchange maintains Emergency Operations Centers (EOC) at both the primary and backup sites. Should an emergency affect the primary site only, an additional temporary location has been made available through a local community relationship. Each location is prepared with cable TV service, whiteboards, copies of the CMT plans, computers, as well as digital and analog phone service.

Maintaining communication is the single most important aspect of any emergency recovery effort. All aspects of our emergency operations are choreographed via multiple communications links between resources and the Exchange's responders, and are coordinated and managed using a wide-array of communications tools. Continuity planners must envision and plan for emergencies that disable telecommunications, utilities, transportation, other infrastructure service, vendors, and customers.

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

Disaster Recovery

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

No planner can accurately predict emergencies they may face or the constantly changing effects generated from a disaster. We must provide multiple ways for our team members and critical staff to communicate during an emergency. Providing good communication tools and alternates allows our organization to respond to any problem encountered and also provides the critical ability to change course as the emergency response requires and to immediately communicate those changes to the Exchange community.

The Exchange information technology systems form the underpinnings of our ability to recover the services we provide to the marketplace in a timely fashion. As new systems are deployed at NYMEX, fault tolerant, distributed, active-active, and advanced replication technologies are used to help ensure that we can provide these services in the most adverse environments. We have recently completed projects to replicate our storage area network to provide real-time duplication of critical back-office information to the disaster recovery site, making this information immediately available both locally and remotely. We are preparing to roll-out an upgrade to our Virtual Private Network (VPN) system allowing remote control of systems and access to information from the distributed remote offices. We have completed a project deploying Digital Access Cross Connect (DACS) equipment in our disaster recovery site, which will enable us to instantly and remotely transfer dial tone and private lines from our primary site to our backup site, utilizing our dark fiber network.

Continuation of our training, education, and awareness program and quarterly testing ensures that the systems and staff are ready to respond to a disruptive event. The EOT meets regularly via a dedicated conference call bridge to discuss continuity planning, updates, and changes in business processes. Regular awareness meetings are conducted with the CMT for retraining and table-top exercises.

Testing

In September 2004, NYMEX testified before the House Financial Services Committee hearing on the emergency preparedness of the financial services sector. We have since participated in the TopOff III exercise sponsored by the U.S. Department of Homeland Security, which was designed to test the readiness of first responders, federal, state, and local emergency managers, along with key infrastructure components such as hospitals and transportation networks. The securities industry component of the TopOff III exercise involved the SEC, the U.S. Treasury Department, exchanges,

and trade organizations such as the Securities Industry Association, Bond Market Association, and the Futures Industry Association (FIA).

In addition, in October 2004, NYMEX, the FIA, other leading futures exchanges and clearing firms successfully completed the first ever industry-wide disaster recovery test. The test scope has expanded in 2005 to include market data vendors. This industry-wide disaster recovery test has become an annual event and is scheduled for October 15.

Industry and Government Coordination

The Exchange is among the leaders in an industry-wide initiative to standardize the protocols governing the way companies send and receive data. This will help many companies develop systems based on standardized specifications, making it easier to deploy and maintain data communications internally and externally under challenging circumstances.

Our industry relies on a complicated inter-relationship of many companies and services. Successful recovery of the financial services sector depends on the quality and thoroughness of extensive planning efforts across many inter-dependent industries. NYMEX uses opportunities such as the futures industry test to go beyond its business boundaries and work together with a wide-array of outside parties to effect communications and business continuity awareness.

Another area we have taken advantage of is information sharing alliances. The Financial Services Information Sharing Analysis Center (FS-ISAC) is a source of critical information ranging from information security alerts to homeland security threat analysis. The New York City Office of Emergency Management is another source of information for New York-based companies. This information is critical for the constant monitoring of potential disruptive events.

Conclusion

NYMEX has a global presence. The Exchange's energy and metals futures markets provide benchmark pricing information that is used worldwide. NYMEX recently opened an exchange in London and signed a joint venture agreement with the Dubai Development Investment Authority (DDIA). The Exchange must be cognizant of world events.

NYMEX views continuity planning as an on-going project that is necessary to meet critical business needs and has incorporated this planning into its day-to-day operations. Every project, system, or business process deployed incorporates some form of continuity planning.

Risk and impact analysis, training, disaster recovery testing, and regular meetings with critical staff create a sense of awareness throughout the company; business continuity planning has become part of the NYMEX business fabric.

We strive to learn from past experience. The 9/11 terrorist attacks, the 2003 blackout, our mock disaster testing, and planning for the 2004 Republican National Convention have helped us prepare for the future. This year as we were finalizing preparations for the launch of the London trading floor, we activated our emergency teams as a response to the July 2005 transportation bombings in London. We are currently following important developments in the Gulf Coast region as our nation struggles with the catastrophic damage caused by hurricane Katrina. Monitoring such disruptive events helps us to adjust and improve our planning accordingly.

Government agencies are of critical importance in planning for and providing support during an emergency. The relationships the Exchange has developed with important government leaders has enabled us to overcome many difficult recovery challenges. In the immediate aftermath of 9/11 we received significant assistance from the federal, state, and city governments.

This year NYMEX has taken advantage of the Business Network of Emergency Resources (BNet) Corporate Emergency Access System - a joint effort between local government emergency planners and private business. BNet provides a special access card that allows a limited number of key critical staff into restricted areas for the express purpose of sustaining crucial business operations.

The Exchange appreciates being invited to participate in these importance discussions. Further efforts to improve communication with our government will only strengthen the ability of the nation and the financial markets to respond to the challenges that lay ahead.

Large scale emergencies similar to those that have occurred in the past are inevitable. Continuity planning is not an individual task, but must be faced by all involved participants in the financial services sector.

I would like to thank the Chairman and the members of this committee for holding this hearing and inviting NYMEX to discuss this extremely important topic.

Mr. PLATTS. Thank you, Mr. Gaer.
Mr. Randich.

STATEMENT OF STEVE RANDICH

Mr. RANDICH. Thank you for allowing me to testify today. I'm Steve Randich. I oversee operations and technology at the NASDAQ stock market, which is the largest equities market in the world. It's always been a priority at NASDAQ to maintain a hardened resilient operation that can withstand catastrophic events. A few principles I want to communicate today is that NASDAQ for a very long time has viewed business continuity and disaster recovery as a top priority. We've had a backup data center in a remote geographic location for 20 years.

Second, exchanges in the United States are evolving toward an electronic trading model and this will naturally enhance the capital markets' ability to withstand catastrophic events. Last, business continuity planning is a collective effort. A stock market alone does not represent our capital markets. Instead, it is only as good as its weakest link.

Our operating model provides a natural business continuity advantage. Historically, an exchange operated at a central physical location where buyers and sellers would meet face-to-face to trade. A single central location without a practical and tested capability of backup puts our Nation's capital markets at risk. Trading at NASDAQ is executed through our sophisticated computer and telecommunications network. Unlike physical floor-based exchanges which employ a specialist to direct buying and selling of a stock, NASDAQ's open architecture structure utilizes hundreds of geographically diverse and competing market makers who simultaneously provide trading liquidity for stocks listed on the market. This insures not only healthy competition for investors, but, more importantly, prevents a single point of failure given the geographic diversity of these market makers.

NASDAQ was prepared for and fully resilient operationally to September 11th and the blackout of August 2003. Geography is critical to our operation resiliency. We have two data centers that are more than 300 miles apart. They are located in different geologic and climactic zones and are in different regional power grids outside of metropolitan areas. We store enough fuel onsite to allow us to run our data center for a full week during an extended power outage without a refill. We also maintain 185 tons of batteries for additional backup. We test each of our generators weekly and perform a utility failure test across the entire infrastructure every quarter.

In addition to geographic diversity, we also use locally situated systems and networks to achieve resiliency. Several network providers are utilized, each with network diversity conductivity into our two data centers. Market participants are insured maximum protection by employing diverse access to both our primary and backup data center at all times. At no time during the week of September 11th were NASDAQ systems inoperative. When the attacks occurred, trading was suspended, but NASDAQ's systems and network continued to operate. We focused on insuring connectivity to our market participants who provide liquidity to our marketplace.

Although actual stock trading was suspended, our systems operated continuously throughout the week.

Notwithstanding the success after September 11th NASDAQ implemented improvements to our backup system. We added more frequent testing to our backup site and began regularly testing full market-wide disaster recovery tests that are open to all market participants. In collaboration with State and Federal authorities, we evaluated and increased our physical security.

Although large portions of the northeastern United States were out of business during the blackout of August 2003, NASDAQ maintained full operations throughout that 2-day period. Our alternative power systems automatically provided immediate continuity so that there was no impact. However, the blackout revealed some areas of weakness in the financial sector that required vigilant attention. There's a need for more backup facilities outside of high risk metro areas like New York. Although most large market participants and telecommunications providers had backup systems and procedures in place, they didn't all work as expected. There were several examples of backup generators that failed within 12 hours of the blackout, largely because of either poor fuel quality or machine maintenance.

Looking forward, and since September 11th, NASDAQ has worked closely in participation with the Federal Government and private sector to strengthen the resiliency of our infrastructure. We now have a contingency plan that provides NASDAQ the ability to trade all New York Stock Exchange stocks if its trading floor becomes inoperative for an extended period of time. Nearly 18 percent of the daily NYSE volume already trades electronically on the NASDAQ network, so this contingency trading plan is in effect tested daily.

In conclusion, NASDAQ is continually anticipating, evaluating, preparing for what may occur 1 day. Our preparedness will never be 100 percent perfect as we're limited by our human imagination of what might occur. Our increasingly decentralized, geographically diverse operating model continues to provide us with a high degree of confidence that we will be prepared for the next event. As I said earlier, the industry is rapidly moving toward electronically trading, which is very good news for resiliency. With electronic trading, an exchange no longer needs to be tied to a single location. Effective backup and redundancy is the key to security against any form of accident or attack and essential for our financial national security. For financial markets we believe this is the core lesson of September 11th and the blackout. For the committee and all concerned branches of government, we believe it is a crucial lesson as well.

Thank you for the opportunity to testify today.

[The prepared statement of Mr. Randich follows:]

Testimony of

Mr. Steven J. Randich
Executive Vice President of Operations & Technology
And Chief Information Officer
The Nasdaq Stock Market

Before the House Government Reform Committee
Subcommittee on Government Management, Finance and Accountability

On Financial Services Sector Preparedness
in a Post 9/11 Environment

September 26, 2005

Thank you Chairman Platts, Ranking Member Towns, and members of the Subcommittee for inviting me to testify before you today to discuss the financial sector's preparedness for wide-scale disasters or disruptions. Congressman Towns, it is a pleasure to appear in your district today at the Brooklyn Law School. We greatly appreciate this Subcommittee's interest in oversight and preparedness. Events which have occurred over the last few years – terrorist attacks, power grid failures, and hurricanes – all remind us that those who own and manage critical infrastructure must be prepared to provide continuous service through whatever may come and maintain plans for disaster recovery.

On behalf of the nearly 800 employees of the Nasdaq Stock Market, I am proud to say that it has always been our highest priority at NASDAQ to maintain a hardened, resilient operation that can withstand catastrophic events. I am the officer responsible for the operations of our market and for maintaining our business continuity plans. I can tell you firsthand that we have devoted all necessary time and resources, and have worked

cooperatively with investors, listed companies, our market participant customers, and the government.

If I were to emphasize just a few basic principles at the outset, they would be as follows:

(1) NASDAQ and our nation's other capital markets are a critical national infrastructure. It is imperative that we take this responsibility seriously and be prepared to operate at all times. NASDAQ views business continuity and disaster recovery as critical top level priorities.

(2) Following NASDAQ's lead, the exchange model in the U.S. is evolving towards electronic trading, and this will enhance naturally the capital markets' ability to withstand catastrophic events.

(3) NASDAQ believes that business continuity planning is a team effort. We need to work cooperatively with the industry, investors, and the government. A stock market alone does not represent our capital markets; instead it is only as good as its weakest link.

(4) Finally, America needs to remain steadfastly on guard for natural or man-made disasters, but this Subcommittee and all Americans should know that NASDAQ and the other participants in our industry understand our critical role in the nation's economy and are prepared.

NASDAQ's Market Structure

At the outset, I want to emphasize that NASDAQ's operating model provides us with a natural and tremendous business continuity advantage. Historically, an exchange

operated in a central physical location where buyers and sellers or their representatives would meet face-to-face to trade. Given the challenges our country now faces, an exchange with a single central location without a practical and fully tested capability of backup and related continuity planning puts our nation's capital markets at risk.

In contrast, NASDAQ was created in 1971 by the National Association of Securities Dealers, at the behest of the Securities and Exchange Commission, to use computers to collect and display quotation information in the over-the-counter market. From these rather humble beginnings, NASDAQ has become the second largest equities market in the world in terms of the number of listed companies, overall trading volume, and trading value; and, we are a global leader in using technology to revolutionize the way equities are bought and sold.

Trading at NASDAQ is executed through our sophisticated computer and telecommunications network. Today, NASDAQ connects thousands of traders in hundreds of firms dispersed throughout North America. Data is received from more than 350,000 terminals and workstations and more than 2 million users in 83 countries have access to screens displaying NASDAQ data. On a typical day, NASDAQ's systems process 37 million stock price quotation updates, 88 million buy and sell orders, and 5 million trades. We handle processing peaks in excess of 25,000 transactions per second and maintain less than $1/100^{th}$ of a second transaction processing time, all with greater than 99.99% uptime for our trading systems. Recently, InfoWorld Magazine named

NASDAQ as 36th among the top 100 companies for information technology achievements, and 5th among financial services companies.

Today, NASDAQ lists the securities of over 3,200 of the world's leading companies, representing the entire spectrum of the U.S. economy—from information technology and telecommunications to agriculture, manufacturing and finance. NASDAQ's "open architecture" market structure places virtually no limit on the number of market participants that can provide liquidity on NASDAQ and imposes little geographical restriction on where these market participants are located.

Unlike its physical floor-based peers, which employ a single specialist to direct the buying and selling of a company's stock, NASDAQ utilizes hundreds of geographically diverse and competing market makers who provide the trading liquidity for each security listed on our market. As an example, today there are exactly 134 registered market makers providing liquidity to support the trading of the Microsoft Corporation (symbol MSFT). This not only ensures a healthy competitive environment for investors, but also prevents a single point of failure from a business continuity standpoint given the geographic diversity of our market makers. The NASDAQ model also provides within its market model open access to all alternate trading systems, including ECNs, or Electronic Communications Networks. These ECNs provide electronic facilities that investors can use to trade directly with each other and, in addition to providing a competitive trading environment, extend the geographic diversity and resilience of the NASDAQ model beyond the aforementioned market makers to trade execution venues.

The rest of the world's capital markets have adopted the NASDAQ model, but in the United States the other exchanges have been slow to move away from the floor-based open outcry system. This is now changing, as investors have demanded better, more efficient systems and the Securities and Exchange Commission has adopted a new rule, Regulation National Market System ("Reg NMS"), to encourage electronic trading.

NASDAQ and Business Continuity

Today, NASDAQ sets the standard for excellence in industry-wide terrorism preparedness and contingency planning. The outcome of NASDAQ's long standing planning, investment, implementation, and testing of continuity initiatives has been evident in all recent events. NASDAQ was prepared for, and resilient to, the events of 9/11; our systems remained fully operational throughout the week although we chose to close after consultations with the government and industry. NASDAQ was also prepared for, and resilient to, the blackout of August 2003 when the northeast power grid failed. NASDAQ's resilience during such large scale events is due in part to our focus on ensuring that redundancy backup and geographical diversification are an integral part of our operation.

NASDAQ has offered strategic guidance to both the government and the private sector. In addition, the FBI, Navy, various military officials, our market participant customers and, most recently, the Secretary of the Treasury, have toured our technology facilities to

learn from us about continuity and disaster recovery. We are proud to meet this responsibility to help secure America's financial markets against a catastrophe.

I would now like to discuss NASDAQ's operating model and business continuity plans in more detail. Thereafter, I will highlight lessons learned from these catastrophic events and how we prepare for unknown events.

First, geography is critical to NASDAQ's operational resiliency. We have two data centers that are more than 300 miles apart. Our Northeast Data Center in Connecticut has been in operation since 1971, and our mid-Atlantic Data Center, which until recently was located in Maryland, has been in operation for 17 years. This data center was moved in September 2005 to an undisclosed location further from Washington D.C. that better satisfies our requirements for security, resiliency, and geographic diversity.

Our geographic diversity minimizes the risk of a single catastrophic event impacting both of our data centers. The data centers are located in different geologic and climatic zones and are on diverse regional power grids. Our primary data center is housed in a rural corporate park, where we have two diverse utility power feeds and are permitted to maintain 35,000 gallons of diesel fuel on-site – something we could not do in Manhattan. This fuel permits us, in the event of an emergency, to run the primary center on four 1,500 KW Detroit Diesel generators that can be powered for a full week without a fuel refill. We also maintain 185 tons of batteries for additional back-up. We test each of our

generators weekly, and perform a utility failure test across the entire infrastructure every 90 days.

It is NASDAQ's view that, in addition to what is accomplished through geographic diversity, resiliency must also be achieved with locally situated systems and networks. From a telecommunications perspective, NASDAQ utilizes several extranet/network providers, each with diverse network connectivity into our two data centers. Market participants have the option of selecting one or more of these providers, ensuring maximum protection. By design, each of these market participants has diverse access to our primary data center, and also has automatic diverse connectivity to our backup data center, a design which maximizes the likelihood of operational continuity of our market following a widespread event.

9/11 And Its Aftermath

Immediately following the tragic events of 9/11, NASDAQ evaluated the extent of any damage to our system and our market participants, and set about determining the necessary steps to reopen the market. In so doing we were guided by four principles: First, we would do nothing that impeded the rescue effort. Second, we would closely coordinate all our activities with the SEC. Third, we would open our market only when major market participants were fully prepared and, preferably, simultaneously with other markets. Finally, in this crisis we would reach out to and assist our members and issuers, just as we do every day.

These principles were widely shared and contributed to the suspension of trading in all markets for four business days. However, at no time throughout the week of 9/11 were NASDAQ's systems inoperative. At the time of the attacks, trading was suspended but NASDAQ's systems and network continued to operate. As a result, our primary concern was focused on our ability to connect to firms that are active in our marketplace and bring liquidity and order flow. In fact, NASDAQ's systems continued to operate throughout the day of 9/11 to allow firms to access our systems so that they could reconcile their books and straighten out their affairs, and for mutual fund pricing and other activities to be completed properly. Although actual stock trading was operationally suspended, NASDAQ's systems operated continuously throughout the rest of the week for this purpose and to allow firms to test connectivity in preparation for the resumption of trading on September 17th.

In the week that followed, NASDAQ worked closely with all participants including the government, each of the equity and options exchanges and our own market makers, ECNs and the over 4,000 companies that listed their shares with us at that time. All told -- and working around the clock -- NASDAQ employees provided technological support to over 800 NASDAQ and non-NASDAQ participants in the financial services industry, domestic and foreign. We consider it a national triumph that trading resumed on Monday, September 17. We are grateful to the many institutions and individuals who made that happen and we are proud of our role in the process.

Notwithstanding this success, after 9/11 NASDAQ identified and implemented improvements in our backup systems. We added more frequent testing to our backup site. Testing, which had been quarterly, was increased to monthly and we now selectively invite market participants to take part. Annually, we also host a full market-wide disaster recovery test that is open to all NASDAQ market participants. During a recent industry-wide disaster recovery test, market participants representing 75% of our daily share volume tested successfully. In collaboration with State and Federal authorities we also evaluated and increased our physical security by broadening the buffer zone around our data center; implementing a fingerprinting policy for all employees and contractors; establishing a separate facility for receiving, x-raying, and opening all U.S. and commercially delivered mail and packages; implementing a single facility entryway with body and personal effects x-ray screening; and increasing the security access credential requirements to all data center buildings, including biometric readers for access control to the computer rooms.

2003 Blackout

Just two years later came another test: the blackout of August 14, 2003. The blackout again proved the worthiness of our ongoing contingency planning and testing. Although large portions of the northeastern United States were out of business, NASDAQ was fully operational during the blackout. NASDAQ's alternate power systems automatically provided immediate continuity so that there was no impact on our operations for the day. All infrastructure systems functioned as designed and seamlessly supported the full operation of our trading systems and networks at our primary data center site. As well,

NASDAQ's backup site remained unaffected, validating our geographic diversification strategy. For Wall Street, trading resumed the morning after August 14. Most firms were able to access their backup sites and were well prepared for business continuity.

The Blackout revealed some areas of weakness in the financial sector that need ongoing attention such as the need for further geographic diversity and more redundant telecommunications systems. There is a clear need for more back-up facilities outside of high risk metropolitan areas like New York City. We also noted that although most large market participants and all telecommunications providers had back-up systems and procedures in place, a lack of robustness and routine testing and maintenance revealed a substandard level of achievable resilience. For example, there were several examples of back-up generators that were immediately activated when the power failed but eventually failed within the following twelve hours because of poor diesel fuel quality or machine maintenance.

Looking Forward

Since 9/11, NASDAQ has worked closely in partnership with the Federal government and the private sector to evaluate our industry's strengths and weaknesses and to continue to strengthen the resiliency of the nation's financial infrastructure. We participated in the GAO's study that resulted in the February 2003 report to congressional requestors on "Potential Terrorist Attacks – Additional Actions to Better Prepare Critical Financial Market Participants." We have also testified on numerous occasions.

One example of this strengthening is NASDAQ's announcement of a contingency plan to trade NYSE-listed stocks if the NYSE is ever unable to operate both its primary and backup systems. After 9/11, the SEC requested that NASDAQ and the NYSE develop plans to provide a reciprocal trading capability in the event of an emergency. After consultation with the SEC and months of preparation, NASDAQ is now able to trade all NYSE and AMEX stocks if their respective trading floors were rendered inoperative for an extended period of time. In effect, in the event of a catastrophic New York metro emergency, NASDAQ is fully capable of trading all 6,700 U.S. Securities listed on NYSE, AMEX, and NASDAQ on our geographically diverse and resilient network. NASDAQ currently provides its market participants on a daily basis the ability to trade all NYSE- and AMEX-listed stocks electronically on the NASDAQ network. Today, nearly 18% of the overall daily NYSE share volume is traded on NASDAQ in this manner. We are the 13th largest volume participant accessing the NYSE floor today. The point here is that NASDAQ's reciprocal trading capability is operationally in effect on a daily basis. Regulation NMS is expected to dramatically increase the electronic trading capability of NYSE stocks, further enhancing the resiliency of our capital markets.

Conclusion

NASDAQ is continually anticipating, evaluating, and preparing for what we expect may occur one day. I must note that our preparedness will never be 100% perfect as it will tend to be limited by our human imagination of what might occur. This process is continuous and dynamic, and as time progresses more complete in terms of increasing our ability to withstand the unexpected. Our increasingly decentralized, geographically

diverse operating model continues to provide us with a high degree of confidence that we will be prepared for the next event.

I would like to conclude by discussing briefly the preparedness of our capital markets in general, both in the past four years and today. The key point is the crucial importance of redundancy, geographical and otherwise. NASDAQ avoided disaster in '01 and '03 not by hardening any single point of failure, but by redundant systems and networks both locally and with geographic diversity. Our resilience to catastrophe lies in our geographically decentralized network and our several levels of redundancy. Although the recovery of America's financial markets was extraordinary after 9/11, there is a need for more back-up facilities outside high-risk environments such as New York City. Stronger telecommunication systems are also critical.

The other major point here is that the industry is irreversibly moving towards electronic trading, and this is good news for resiliency. With electronic trading, an exchange need no longer be tied to a place. Rather, it can be maintained redundantly in multiple places and run by multiple systems, and redundancy is the key to security against any form of accident or attack. What is best for investors and for markets overall is also best for our financial and national security. For financial markets, we believe this is a core lesson of 9/11 and the blackout. For the Committee and for all concerned branches of the government, we believe it is a crucial lesson as well.

Thank you again, and I welcome any questions you may have.

Mr. PLATTS. Thank you, Mr. Randich. Again, to all of you, appreciate your testimonies.

Maybe a broad question to each of you, just in dealing with the Federal Government in your respective organizations and members; infrastructure, critical infrastructure protection, what do you see as the greatest hurdle in dealing with preparedness and is there any specific statutory changes you believe need to be made to allow better cooperation, interaction with the Federal Government? If anyone would like to——

Mr. DONAHUE. I'll start. Mr. Chairman, I certainly could not recommend any statutory changes, although some of my co-panelists may have ideas. I think we, as you unquestionably heard this morning in the testimony, the financial sector is very, very proud of what they have accomplished in this space and I think rightfully so. There has been a lot of energy devoted to this.

You asked earlier about the state of compliance with respect to the sound practices paper. All of our organizations have met their deliverables by this time. The significant firms in the paper are all well on track to meeting the deliverables by 2006. I think our interaction with Government in support of those objectives has been very positive. I think a question that looms on the horizon is, speaking personally, how much is too much and how much do you achieve agreement in the public and private sectors about the degree to which resource investments yet need to be made in financial services to achieve levels of resilience beyond where we're at at this point, and making sure that we all have a very reasonable sort of judgment. If we can arrive at a reasonable judgment on that question is going to be a key issue as we go forward.

Mr. PLATTS. Cost benefit analysis——

Mr. DONAHUE. Very, very much so. Again, you heard from all the remarks people were making, that there have been a significant investments by a number of the industry infrastructure members and a number of individual firms, and making sure any additional adjustments we're asked to make by the benefits we're going to derive from them is a critical issue going forward.

Mr. PLATTS. Ms. Allen.

Ms. ALLEN. I would say the two areas I would like to see the government spend much more time focusing on is the interdependency area to understand how dependent we are on these other critical sectors, and how much our regulators can require us to do something. We cannot do it if the telecom, power industry and IT industries are not there, and we must place the focus on cyber security.

Second, I don't know if there are statutory changes needed, but an example would be antitrust exemption. BITS has a product certification program. It's a voluntary testing program by vendors, software vendors, to meet minimum security requirements. They overwhelmingly tell us, "We really aren't going to do it unless we're mandated to do it." BITS cannot mandate because of antitrust concerns. So, look at how do we as an industry or even critical infrastructure industries set standards for cyber security.

Another thing is, again, incentives for the telecommunications infrastructure to have alternative telecommunications systems, but also to provide this diversity of redundancy that we need.

Then last, I think the concept of funding regionals was brought up. If there were some kind of seed money that would help, we would—let's put it this way, it would happen much faster, if there were some seed money for the critical areas. We could all sit here and name who were the 10 to 15 critical geographic areas and there were some seed money. There's a model, there's some support, but it does take money, it takes some coordination to implement.

Mr. GAER. I would actually echo some of the statements made regarding to—our experience regarding government involvement with disaster recovery business continuity has been a very positive one, in the fact that we're regulated by CFTC is our primary regulator. I took this job beginning in March 2003 and we were planning for a lot of these industry-wide events that were going to occur because the exchanges all got together, at least in the futures industry the exchanges all got together and said what do we have to do to make this work a little bit better. It was very refreshing to see representatives from the CFTC attend these meetings and say, listen, we're going to let industry drive this process, we're going to let industry drive the process, we're going to stand back and watch and see how you're doing it. We don't want to have to step in, so please manage this correctly.

From all accounts, from everything you've heard today, I think the financial services industry as a whole has been managing it very well. Interaction with government has been on a very open basis, our access to things like GETS cards for critical personnel to use, Government Employee Telecommunication Service, I think it's called? Government Emergency Telecommunication Services. NYNEX's interaction with the OEM for events such as Hurricane Isabelle of last year, where we're invited to come and join in government and to work together in partnership with government, but it's very clear from our experience, our industry-wide test, the blackout of 2003 that industry is going to drive the acceptance and industry is going to drive basically the ultimate result of any disaster recovery model.

Mr. RANDICH. Briefly, having worked in a number of industries, I find it amazing how this particular industry is so self reliant and motivated in this regard, which is a good thing. So in that area, I really don't see any need for any specific legislation, only facilitation of policymaking that encourages technological innovation and solution in the area of business continuity and disaster recovery.

Mr. PLATTS. Thank you, and I think this industry has gotten the American way of what do we need to do and how do we need to do it and let's get it done. I think that's been reflected in all our accounts today, the aggressive nature.

That being said, I think one of the challenges for the industry, I think everybody has touched on it in some way today, is the interdependence of your industry with these other critical infrastructures; telecommunications, power, transportation, you name it. What would be your read on your interactions with these other sectors, if you want to pick power specifically, communication, and how they're responding and I think it was, Mr. Randich, in your testimony, about how they have onsite generators for a week's worth of power, fuel, if we had here in your facility like in New Or-

leans, where not only it's going to be well over a week before power will be restored, it's going to be months to some of those areas, and even inability to get transportation in because of the amount of damage that was done, how is the energy industry responding to having an ability to be redundant in their provision of services as best possible to your needs, again, not just energy, any of the infrastructure industry that we depend on.

Mr. RANDICH. In all cases, the answer is never going to be perfectly. However, we all have choices that we make in the marketplace. We decided where we want to put our data centers. We decide who we're going to buy fuel from. We decide who is going to be our network provider and our power provider and we make those choices, so there's some vendor diversity, as well as we pick partners that have proven to be reliable over time. So I very much believe that the free enterprise economics and decisionmaking over time converge on the best solution for the markets that eventually prevail.

Mr. PLATTS. As much as possible, again, market-driven solutions.

Mr. RANDICH. Market-driven solutions.

Mr. PLATTS. Ms. Allen.

Ms. ALLEN. I would add that the telecommunications industry has been very helpful. Much of that from the work of Duane Ackerman, who chairs the NSTAC, the President's Advisory Council. In the private sector, CEOs and CIOs from the telecommunication sector work closely with us on that. It has come less from the government other than the NCC.

The telecommunications, the best practices we're working on there, includes how many days of backup fuel you need to have, what are the transportation sources for that. That is, again, a private sector-led effort. It's not to say that the Department of Energy and others aren't doing things in this critical infrastructure area, but it tends to be more focused just on the industry, less on the interdependency issues.

Mr. PLATTS. OK. How about in the sharing of information through the ISAC process and how that's working and specifically with financial sector, you're read on where we are and where we could go to insure that's effective in its intent?

Mr. DONAHUE. I think the sharing of information for the ISAC has been very successful to the extent it's reached. We're building the interstate highway at this point, and we are building a communications infrastructure that can get information out to members of the sector. We, obviously, have some distance to go in terms of adding end points to that network, but I believe that has been very successful and I think the ISAC membership is finding it very useful to get the alerts and the information that comes to them through that channel.

I think Jim Caverly in the earlier panel put his finger on where this needs to evolve, which is the development of more formal procedures for information coming from the private sector to DHS, to Treasury in its role as sector specific agency about where we believe vulnerabilities continue to exist.

Involving the private sector picture, conversely, of opening channels information from government in terms of threat information, in terms of more sensitive information of where clearance is pos-

sibly going to have to be obtained in order to be able to do that. That's the area that needs work and experimentation.

Mr. PLATTS. That was actually one of my specific questions, because in your testimony you talk about the importance of communications and information, but what's your read on that access to sensitive information, whether security clearance is being required? Sounds like we have a ways to go in allowing that to be a more seamless automatic process.

Mr. DONAHUE. I don't think anyone is comfortable with the state that has reached. DHS and Treasury both working together did sponsor members of the FSSCC for clearances at the secret level, which has been very helpful. I think there have been instances where information could be discussed on conference calls where we knew everyone on the call had a particular clearance and therefore they were somewhat more free to discuss matters, but it's clear that we don't understand who all needs to have access to the information, how do you sanitize information so that you can be conveying it to people who aren't necessarily cleared. I mean, all of those issues still have to be explored.

DHS approached the FSSCC in I would say late spring and asked for our agreement to work with them on the development of an information sharing pilot that would sort of go to the next generation of an information sharing methodology between the government and the private sector. We have agreed with them to go forward with that and I think Katrina and Rita have intervened to sort of put that on the back burner for the moment, but I'm sure that will be something they return to in the fall.

Mr. PLATTS. The interaction I guess between the private sector and the government, what is specifically in New York, if there is a major incident, what's the process of structures in place for yourself, your organization or members as far as being in touch with the New York City emergency response office, the NYPD? Is that a very formalized structure that you have a contact, people that you go to, and if one of the things that's down is communications, how do you make that contact, even if you have the right person to be in touch with?

Mr. GAER. For us, our proximity is probably one of our biggest assets in that situation. We have both formal and informal ways that we communicate with government here in the city as well as regional and national government. We're briefed on an ad hoc basis as far as threats and threat levels, especially ones that are germane to the financial services area. I think it was about a year or so ago when there were threats against Merrill Lynch and I think it was Prudential in Newark, where we were advised of these threats ahead of time and we were able to harden beforehand. We interact with local law enforcement, the Joint Terrorism Task Force, very well, as a matter of fact, sometimes to almost the shock of visitors who come to our facility in the rigorous amount of security that's around the building and how they have to get into the building, they're very, very shocked and then later impressed at how secure we keep the building.

But the communication between ourselves and between government, again, it's formal and's informal on an as-needed basis. I have a list of contacts, our president, our chairman, the crisis man-

agement team can get in touch with people at their homes on their cell phones or what have you, so it's been a very post September 11th, it's been a very kind of open cooperative environment.

Mr. DONAHUE. A number of the infrastructures in New York, you mentioned that you have a seat at the OEM, others do as well. In the event of an emergency in this city, we know that our people are supposed to go to OEM. Security Industries Association has a seat, my organization has a seat, the Exchange's technology arm has a seat. People know they're supposed to immediately go there so they can be part of that centralized communication.

You mentioned GETS cards earlier, there has been a fairly wide distribution of GETS card within the financial infrastructure in the country, certainly in New York, so people have the ability to communicate if any telecommunications are available they get priority. The city has implemented a corporate emergency access system where we have cards that will give us access to no-go zones, for example, as I'm sure you know. Post September 11th, south of Canal Street people were not allowed to come for the first few days. This program would allow us to get people into our facilities and get things working, even though it might be in an area ruled not open to the public. So there are a number of steps the city has taken to improve communication and coordination that way.

Mr. RANDICH. That privileged physical access is a huge improvement since September 11th.

Mr. PLATTS. Is it fair to say with the physical access or the seat at the table with OEM, that this is since September 11th, this is lessons learned and then since the blackout to keep kind of honing each incident and get a little better?

Mr. GAER. Yes.

Mr. DONAHUE. Absolutely.

Ms. Allen. Those are lessons that have gone to the original coalition, ChicagoFIRST and other models as well.

Mr. PLATTS. Your work with the creation of ChicagoFIRST really was a lot of that was derived from New York, we were talking earlier——

Ms. ALLEN. Right, the lessons learned from September 11th and we spent time with the OEM of New York because New York was actually ahead of all other regions and we used their model and shared back with them what we had developed on the regional model.

Mr. PLATTS. Thank you.

Mr. Donahue, in your testimony you talked about participating in the TopOff 3 drill. I'm sorry, Mr. Gaer, sorry. And you referenced that and all the different participants. What I was curious, your read on how successful the exercise was from the standpoint of, again, lessons learned and what would work or not, and how you responded to the exercise in implementing the lessons learned.

Mr. GAER. I think you can only judge how successful an exercise is by its objectives and I think for these particular tests the objectives being that you had so many participants from diverse areas, you couldn't really go through every permutation of everything, so to speak, that's going to happen. We actually judged it from our point of view to be very encouraging, to have been very successful. Where we are right now is honing in on our industry-wide disaster

recovery test, although it's not going to include the telecom sector per se or the power sector per se. We're really working in our industry to get it right in our industry first and our first test last year was a very kind of bland, basic test which was very successful and it actually exceeded people's expectations and there was a lot of discussion prior where you get everybody on board as to when you can do it and what are we going to do and what are we going to run through and it turned out that people were more prepared than we thought they were going to be.

For the TopOff, the interaction between ourselves and the various other industries and agencies I thought went very well. Certainly in every exercise there are areas where you need improvement and again I would probably highlight, as other members of the panel have, the improvements between the telecom sector and financial services sector would probably be something we should concentrate on.

Mr. PLATTS. A followup to that, Mr. Donahue, was the coming exercise October 15th that you reference in your testimony. Could you walk me through what's going to happen there and what involvement, because you reference sponsors and the various institutions that are going to participate, the involvement of any Federal agencies that will be participating or just kind of watching, taking in that exercise?

Mr. DONAHUE. I think, first of all, what will happen on the 15th is 200-plus firms are going to, there are essentially two tests occurring that day concurrently, the Futures Industry Association is doing its second iteration of its industry-wide test. The securities industry and Bond Market Association are coordinating a test for their members on the cash side, which is the first time that piece of the securities industry has conducted such a test and essentially, what will happen is that each of the participants in the test will go to their backup data center locations and their back up business process center locations and seek to establish connectivity with key industry infrastructures, DTTC being one, the New York Stock Exchange being another. Steve, I don't know if NASDAQ is participating, but NASDAQ would be another infrastructure that they are, I'm assuming you are, and that would be another infrastructure that they connect to. Establish connectivity and run a few transactions through.

We're not going to try to simulate a day's activity or anything like that, but run transactions through so make sure you can get transactions to the trading facility, for example, and then you can get feedback from the trading facility acknowledging receipt of the order, acknowledging execution of the order, whatever it may be, so you can function on your backup if you need to in the light of an emergency take place.

Mr. PLATTS. Is FCC or Treasury going to be in any way participating or watching how it goes?

Mr. DONAHUE. They will be getting a report on the test results after the fact. At this point it is essentially, this is the model the industry followed in preparation for Y2K. We conducted tests that we had organized and we implemented. We were reporting to our regulatory agencies, to Treasury as well in this instance, how that it proceeded, because it's clearly of interest to them, but it's not

something they would have direct involvement in on the actual day of the event.

Mr. PLATTS. I think another good example of the private sector not waiting for government to say, hey, do this, but responding appropriately to being well prepared.

Mr. Randich, in your testimony you went through in detail some of your security preparations from buffer zones around the data center, fingerprinting policy for employees and contractors. A pretty extensive range of security measures. What would be your assessment on how common that is in the financial sector, whether it be specifically here in New York or a broader sense nationally.

Mr. RANDICH. Significantly more so than it was in September 11th, just being in the business and having to go visit our customers and peers. It's like going through the airport several times a day, so that's very good news.

The one area I think is important to note kind of where it's limited and where it would be important to improve, one of the advantages we have is that our two data centers are located in corporate parks, remote areas in one case, even beyond the suburbs. That basically allows us to, where the single owner tenant of the facility gives us 100 percent control over the security and the infrastructure and sometimes I feel that organizations that have their critical assets in a multi-tenant high-rise in the metro area don't have the level of control that they might need.

Mr. PLATTS. Again, in any urban setting your ability to have that, proximity of other buildings, even if it's your own building is a lot more challenging in an urban setting.

Mr. RANDICH. Very much.

Mr. PLATTS. Would any of you like to comment on that issue of the breadth or depth of security in the private sector?

Mr. GAER. I actually could and I'd like to put a little bit of a twist on it in that yes, security, at least from the Exchange level, we have as members virtually every investment bank, large trading house, etc., they're members of ours and we're kind of this hub, or a utility for liquidity and price formation, so we need to take extra steps to be as secure with our—in our physical as well as our virtual presence. But what I'm seeing, what I've seen personally from being in Europe and being in London in particular, London has definitely tightened up security post what they call 7/7, but I will tell you that the security that you find, especially here in the New York metro area is light years ahead of what is happening outside the United States and that's important to us for reasons of cyber security, which I believe is probably going to be one of the next great frontiers that we are all going to have to tackle as an industry in our DR testing.

Mr. PLATTS. I think that interdependence with cyber security, because you can harden a facility, but you could be on the other side of the world and depending on the cyber security protections out there, they can still do great harm, and that's come to light in some of the recent reports on China and some of their—at least what appears to be concerted Government efforts on an incredible scale to break into sensitive data bases in the United States, not just government offices. So that challenge is one that is global and what happens elsewhere is going to impact us.

Is there an interaction with those European markets and what we are doing here in New York? We talked a lot about sharing of best practices here, how much of that is occurring international?

Mr. GAER. I can only speak from our industry and I would have to say very little as far as an international effort, I would say very little.

Mr. DONAHUE. Depends on the level that you're talking about. At the infrastructure level, it's quite a bit. Swift is the international payments messaging network, our counterparts in Europe, Euroclear and Clear Stream are the two securities depositories over there. There are very definitely interactions in those core organizations and what's the best practices we participate in Swift committee, we meet with Euroclear and exchange business continuity standards very regularly.

Once you go beyond the infrastructure, I would agree completely that different firms are not necessarily coordinating the way that we're seeing here in the States.

Ms. ALLEN. We have some BITS members at the Canadian Bankers Association and APACS, which is the payment system in the UK. We've shared best practices with the Japanese, with the Australians with the OECD countries, but it's nothing formal.

Mr. RANDICH. We've hosted walk-throughs of our data center many, many times. We're continually doing it, and it's interesting, not much European interest, but we've had the South Americans, the Asians and even the Middle Eastern and Indian markets come take a look.

Mr. PLATTS. The hope certainly is that as we are in a global economy, that is everywhere and that the lessons being learned here and especially as I've heard loud and clear, the efforts in the Greater New York area really setting a great high standard, high bar for the rest of the country and the world, and the lessons learned now being in Chicago and looking to regionalize elsewhere around the country and ultimately around the world is going to be so important.

Mr. Towns apparently wanted, and he had to leave for another engagement and apologizes that he couldn't stay through your whole participation, but on technology, as technology continues to advance every day, the ability to insure the security of those technological advances, and do you think our technology sector is doing enough to provide security day one when these new products are hitting the market, software and hardware as well, or do we need to take a closer look at what they're putting on the market from a security standpoint?

Ms. ALLEN. I would say there's improvement, and certainly we are working very closely with the largest provider of operating systems and software. We have a set of business requirements and a work plan with them to meet some of the business requirements we have, but it's a longer term process, because you have to change the culture of the United States, actually all of the software industry, in how it's developed, which has been to get it out there fast and let us be the Beta tests for them.

Today we've got to look at those same providers of technology, whether it's the software, the infrastructure, the systems, to really test code much more rigorously, to develop code much more rigor-

ously, to do the testing and to have the safeguards before they bring a product to market. That's that "higher duty of care"—in particular, if it's a provider where they have a dominant share of the market for the infrastructure industries. So I think there does need to be more attention from not only the private sector, but also the government on this area and I think your question is correct. We have to look at this globally, because these players are global players, they're global players and it's going to be—Microsoft tells us that the time between a vulnerability and exploitation of that vulnerability is getting down to seconds now. There's no way you can physically patch all the problems there so it means you've got to change the way you look at technology.

Mr. RANDICH. I think they're coming along slowly. It used to be a product would differentiate itself from the market with function, price, ease of use. Security has clearly been elevated as a measure of decisionmaking factor in the choice. But by no means should any of us believe you could buy security off the shelf. At the end of the day we have to take responsibility for it by choosing the best, most progressive solution members and tying the loose ends ourselves.

Mr. PLATTS. Again, kind of where we started with questions in that American way of partners between public private sector and individual responsibility and in the end doing what you can.

I want to thank each of you and I wanted to give each of you, if there's anything you think you didn't get to highlight or want to touch on to reaffirm, to give you the opportunity before we close.

Ms. ALLEN. I want to thank you for holding this hearing. We feel the more that Members of Congress understand the issues from the private sector perspective, the better it is. We would be happy to educate others in any way we can.

Mr. PLATTS. We've been happy to have the hearings and have your participation as well as the other panelists earlier and it is a great educational process for Mr. Towns, myself and our committee staff and then having that as a resource beyond just our committee, to do a full committee with the other Members.

We're on the same team. We are all part of a functioning economy in coordination, and the financial sector in New York especially, and ultimately receive quality for it.

Please, each of you, don't hesitate to call on us for things you want to share as we move forward in a month or year or whatever that you think we should be aware of. We're always glad to have that feedback so we can partner well with the private sector in what we're doing in Washington.

We will keep the hearing record open for 2 weeks if there's anything from this panel or previous panels to submit for the record.

Again, we thank each of you and wish you and your organization and members great success in your efforts, and this hearing stands adjourned.

[Whereupon, at 1:19 p.m., the subcommittee was adjourned.]

○