

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

Thank you Members of the Committee.

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

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

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

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

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

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

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

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

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

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

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

For the Department itself, matters were slightly different.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Thank you.