

STATEMENT

OF

CATHERINE A. ALLEN

CEO

BITS

BEFORE THE

HOUSE COMMITTEE ON FINANCIAL SERVICES  
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

UNITED STATES CONGRESS

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

OCTOBER 20, 2003

## TESTIMONY OF CATHERINE A. ALLEN, CEO, BITS

### Introduction

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

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

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

### Power Outage Impact

BITS member companies and customers experienced the outage in Detroit, as well as in New York and other Northeastern states with a high concentration of financial institutions. **Bottom line, the financial services industry and our customers fared well. Backup systems worked, alternate communications systems were used, and there was no measurable impact on**

**settlements and payments. There was excellent cooperation and communications among the financial services regulators, Treasury and the private sector.** However, there were “lessons learned” that require follow-up.

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

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

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

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

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

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

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

### **The Interdependency Issue**

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

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

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

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

BITS is addressing **interdependency issues with the telecommunications industry**. BITS has led an effort on behalf of the financial services industry focused on assessing telecommunication vulnerabilities and enhancing recovery. The telecommunications and financial sectors are demonstrating unprecedented cooperation, supported by the National Communications System (NCS) of the Department of Homeland Security (DHS). The NCS and the DHS have been exceptionally helpful in bringing our two industries together to address diversity, redundancy, and recovery. Results of our collaboration include:

- A detailed and confidential assessment of interdependencies in a specific geographic area as a replicable model for other areas
- Best practices in telecommunications and financial industry procurement policies
- Pilots to model the costs of attaining greater diversity and redundancy in telecommunications services to the financial services industry
- Adoption by BITS and Financial Services Roundtable CEOs of the Network Reliability and Interoperability Council (NRIC) best practices in physical and cyber security
- Education of both sectors on the importance of working closely together to identify and address issues

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

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

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

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

## **Recommendations**

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

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

2. **Announce early whether an event is terrorist-related or not.** This information is critical to the execution of crisis management procedures and communications to maintain public confidence.
3. **Establish improved coordination procedures across all critical infrastructures and with federal, state, and local government when events occur.** Coordination in planning and response between the private sector and public emergency management is inadequate and/or inconsistent. For example, a virtual national command center for the private sector that links to the Homeland Security Operations Center would help to provide consistency.
4. **Recognize that the financial sector is driven by its “trusted” reputation as well as regulatory requirements. Other industries do not have the same level of regulatory oversight, liability, or business incentives.** However, we rely on other sectors because of our interdependencies. Responsibility and liability need to be shared.
5. **Recognize and review the dependence of all critical infrastructures on software operating systems and the Internet.** A cyber attack of some kind which impacts communications, SCADA systems or first responder systems would put all of us at terrible risk. Compounding the problem is the lack of security in software development and the current inefficient software patch processes that cause our industry to spend millions of dollars that could be better used for enhancing security and business-continuity practices. This is an alarming issue and critical to protecting the nation’s infrastructure. A clear understanding of the role of software operating systems and their “higher duty of care,” particularly when serving the nation’s critical infrastructures, needs to be explored.

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